OpenZeppelin | security

Origin Aerodrome AMO Strategy Audit

ORIGIN

September 27, 2024

Table of Contents

Summary

Type	DeFi
Timeline	From 2024-09-09 To 2024-09-16
Languages	Solidity

Total Issues	3 (2 resolved)
Critical Severity Issues	0 (0 resolved)
High Severity Issues	0 (0 resolved)
Medium Severity Issues	0 (0 resolved)
Low Severity Issues	2 (1 resolved)
Notes & Additional Information	1 (1 resolved)
Client Reported Issues	0 (0 resolved)

Scope

We audited the OriginProtocol/origin-dollar repository at commit 4345b52.

In scope were the following files:

```
contracts/contracts
├── interfaces/aerodrome
|   ├── ICLGauge.sol
|   ├── ICLPool.sol
|   ├── INonfungiblePositionManager.sol
|   ├── IQuoterV2.sol
|   ├── ISugarHelper.sol
|   └── ISwapRouter.sol
└── strategies/aerodrome
    └── AerodromeAMOStrategy.sol
```

System Overview

Super OETH is Origin's new Liquid Staking Token which combines the rewards of Ethereum liquid staking with additional investment gains from bespoke DeFi strategies. Users can deposit WETH into the Super OETH vault and receive Super OETHb in return. The WETH they deposit is used to generate the returns from the strategies above and users can come back to claim their rewards with the Super OETHb they hold. One of the strategies implemented by the vault is to provide liquidity in Aerodrome's WETH/OETHb liquidity pool (a fork of Uniswap v3) and receive rewards that Aerodrome pays to liquidity providers. This is all on the Base network.

The scope of this audit is this specific strategy, implemented in the Aerodrome AMO (Automated Market Operator) contract. This contract is responsible for interfacing with the pool to provide the strategy's liquidity in the Aerodrome concentrated liquidity WETH/OETHb pool and act in such a way as to ensure OETHb maintains a stable 1:1 peg with WETH. By doing so, the strategy facilitates seamless trading between OETHb and WETH and generates significant additional rewards through the liquidity incentives provided by the Aerodrome protocol in the form of $AERO tokens. These rewards are then reinvested into the liquidity pool, further increasing the yield for OETHb holders.

A core feature of the Aerodrome AMO strategy is its rebalancing mechanism, designed to maintain an optimal balance between WETH and OETHb in the liquidity pool. Market conditions can cause imbalances in the pool, such as shifts in the relative value of WETH and OETHb, and this can affect the efficiency of the liquidity provision. To counteract this, the pool is monitored off-chain and automatically instructs the strategy to rebalance the pool if needed. The nature of the pool (see Uniswap's documentation) also allows the strategy to only facilitate swaps within an acceptable price range (i.e. near the pegged price). The strategy ensures that the pool remains within a set range of WETH share, with a current target of 20% WETH and 80% OETHb, to allow users to swap OETHb with minimal slippage and maximize the efficiency of the liquidity position.

Security Model and Trust Assumptions

During the audit, the following trust assumptions were made about the codebase:

- Origin's Vault correctly manages deposits, withdrawals, minting, and burning of OETHb.
- The governor and strategist are acting with honesty and integrity, having the best intentions for the protocol and its stakeholders.
- The Aerodrome concentrated liquidity pool the strategy interacts with consistently uses WETH as `token0` and OETHb as `token1`, ensuring that all liquidity operations, swaps, and calculations related to the token pair function correctly within the strategy's logic.
- The Aerodrome concentrated liquidity pool, gauge, swap router, NFT position manager and sugar helper function as intended, providing liquidity, correct reward distribution and seamless token swaps.
- The Bridged WOETH Strategy, alongside the oracle it is interacting with to fetch the price of wrapped OETH, are working as intended to ensure OETHb can be redeemed for wrapped OETH and vice-versa.
- The Base Layer 2 network operates securely and efficiently, with no vulnerabilities or outages that could disrupt the strategy's operations.

Low Severity

L-01 Disable Initializers for Implementation Contract

AerodromeAMOStrategy is intended to be the implementation for a proxy contract, meaning all the functions the proxy can call can be called directly on the implementation within its own storage context. Currently, only the Governor, Strategist, and Vault can call any non-view functions meaning we do not see an issue with the implementation contract. However, it is best practice and we do recommend effectively disabling initializing functions explicitly so that future contracts are developed with that habit. Consider setting `initialized` to `true` in the constructor.

Update: *Resolved in pull request #2251. The Origin Protocol team stated:*

> *Fixed by adding the "initializer" modifier to the constructor which initializes the implementation contract. As an additional measure, the governor of the implementation contract has also been set to the zero address.*

L-02 Revoke Approval

The `safeApproveAllTokens` function approves the position manager and the swap router to have complete control over the strategy's WETH and OETHb balances. Many DeFi systems rely on this blanket permission to be given and handled correctly. While it is assumed that the Aerodrome ecosystem will not take advantage of this trust, nevertheless, it is best practice to create ways for this trust to be revoked. Consider adding a method for the Governor to withdraw the approval.

Update: *Acknowledged, not resolved. The Origin Protocol team stated:*

> *We agree that unlimited approvals are generally not a good idea. Though in the case of "AerodromeAMOStrategy", "WETH", and "OETHb", the tokens are never left on this strategy contract before or after a "deposit", "withdrawal", or "rebalance" transaction. For that reason, we do not see it as an additional risk or a sufficient reason to introduce additional complexity into the code that would handle exact token approvals. If we feel something is unsafe, we have the ability to withdraw all funds from the contract.*

Notes & Additional Information

N-01 Code Clarity

Here are some misleading comments we identified during our review:

- The variable `_liquditytoRemove` should be `_liquidityToRemove`.
- In the documentation of the `_addLiquidity` function, the second sentence should be '...when there is no liquidity...' instead of '...when there no liquidity...'.
- In the documentation of the `rebalance` function, 'withdrawPartialLiqidity' should be 'withdrawPartialLiquidity'.

Update: *Resolved in pull request #2252. The Origin Protocol team stated:*

> *Fixed as suggested.*

Conclusion

We audited Origin's Aerodrome AMO strategy contract, which provides liquidity for Aerodrome's WETH/OETHb liquidity pool and collects rewards for market-making. We found the contract to be securely coded, well-integrated, and highly attuned to the market risks associated with this strategy. We are grateful to the Origin team for their willingness to answer our questions and for taking the time to explain the surrounding systems to us. Their support was instrumental in the success of this audit.