Techrate1 Techrate

TechRate

AUDIT COMPANY

COFFIN

Smart Contract Security Audit

TechRate

October, 2021

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn’t say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and TechRate hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

TechRate was commissioned by COFFIN to perform an audit of smart contracts:

- 0x593Ab53baFfaF1E821845cf7080428366F030a9c
- 0x0DeF844ED26409C5C46dda124ec28fb064D90D27
- 0xEb34f9B25Daa1e500950fB471bAACA6e5Ae5e97E
- 0xEF44292fBEC3F96d63cFb3c004c9ec825CFf354f
- 0x605ce7209B6811c1892Ae18Cfa6595bA1462C403
- 0x98e119990E3653486d84Ba46b66BbC4d82f7f604
- 0x226E0FC82Bcf38a0DA32999AD5CdFC40a71903bd
- 0x79D6289FBC968C60dA9BF35320D75F60498AA9ec
- 0x0AA37a35473989e2EF16477171Ea06d8e9cdDe9F
- 0x61Befe6E5f20217960bD8659cd3113CC1ca67d2F
- 0xb09E30A291654a0581742C15B89Bc5cF2BDf57b3
- 0xA193c5f8De21eE49623Adab32AA478dc152A230d
- 0x681A72D6D6b37814047396FAF9c9f1d629c5f5Dd
- 0x53bB001BdC57aE307B35326088eBd655710bC281
- 0x7A16D7F76950E5c0b9F7870e18eE3C0E40fbF707
- 0x775ff1EE26A439bA26c57E2912c2745Ec85Ab807
- 0x26f0f1ECD9fB1741D65099f4952c4e973cdCd50e
- 0xbcB800FE683b9175FF04ec50ad8fE4b1A0782f0b

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Issues Checking Status

	Issue description	Checking status
1.	Compiler errors.	Passed
2.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3.	Possible delays in data delivery.	Passed
4.	Oracle calls.	Passed
5.	Front running.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow.	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Low issues
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	The impact of the exchange rate on the logic.	Passed
13.	Private user data leaks.	Passed
14.	Malicious Event log.	Passed
15.	Scoping and Declarations.	Passed
16.	Uninitialized storage pointers.	Passed
17.	Arithmetic accuracy.	Passed
18.	Design Logic.	Low issues
19.	Cross-function race conditions.	Passed
20.	Safe Open Zeppelin contracts implementation and usage.	Passed
21.	Fallback function security.	Passed

Security Issues

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

1. TimeLock minimum delay

Issue:

- Timelock contracts (except 2 hours) has the same minimum delay value (2 hours).

2. Wrong burning

Issue:

- *(TaxableToken)* The function _transferWithTax() burn amount over transferred value.

Recommendation:

Include burn amount in tax value.

3. Out of gas

Issue:

- *(PoolToken)* The function removePool() uses the loop to find and remove addresses from coffin_pools_array. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.
- *(CoffinMaker)* The functions updatePools() and _updateAllPools() could fail due to block gas limit if the pool size is too big.
- *(Multicall)* The functions aggregate() could fail due to block gas limit if the calls size is too big.

Recommendation:

Check that the excluded array length is not too big.

Notes:

- *(CoffinMaker)* Contract has withdrawal lockup period.
- *(CoffinMaker)* ≈12% mints to dev address, ≈8% mints to marketing address.

Owner privileges (In the period when the owner is not renounced)

- **PoolToken:**
    - Owner and Coffin pools can burn from addresses (with allowance).
    - Owner can add and remove pools.
- **CoffinOracle:**
    - Owner can change period.
    - Owner can initialize contract.
    - Owner can change Coffin, xCoffin and dollar addresses.
    - Owner can change router and bandRef addresses.
- **TaxableToken:**
    - Owner or TaxOffice addresses can change tax policy.
    - Owner or TaxOffice addresses can change CoffinOracle address.
    - Owner or TaxOffice addresses can enable/disable autoCalculateTax.
    - Owner or TaxOffice addresses can enable/disable using_twap.
    - Owner or TaxOffice addresses can enable/disable taxes.
    - Owner or TaxOffice addresses can change taxOffice and taxCollectorAddress.
    - Owner or TaxOffice addresses can include/exclude from taxes.
    - Owner or TaxOffice addresses can change tax and burn thresholds.
    - Owner or TaxOffice addresses can change tax and burn thresholds.
    - Owner or TaxOffice addresses can change static, basis and max tax rates. Also change adjustTaxRateA and adjustTaxRateB.
- **Coffin:**
    - Owner can initialize contract.
    - Coffin pools addresses can mint reward.
- **CoffinMaker:**
    - Owner can initialize contract.
    - Owner can change rewards per seconds.
    - Owner and funds addresses can change their addresses.
- **CollateralReserve:**
    - Owner or gate address can transfer any ERC20 tokens.
    - Owner can change gate address.
- **Dollar:**
    - Owner can initialize contract.

- **Gate:**
  - Owner can initialize contract.
  - Owner can withdraw contract tokens.
  - Owner can toggle minting and redeem.
  - Owner can change oracle, policy and collateralReserve addresses.

- **GatePolicy:**
  - Owner can initialize contract.
  - Owner can change ratio_step, price_target, refresh_cooldown and price_band values.
  - Owner can change dollar and collateral addresses.
  - Owner can change target_collateral_ratio value.
  - Owner can enable/disable using_twap_for_tcr, using_twap_for_redeem and using_twap_for_mint values.
  - Owner can change oracle and gate addresses.
  - Owner can change redemption and extra redemption fees and change redemption delay.

- **TaxOffice:**
  - Owner can change coffin and uniRouter.
  - Owner can call Taxable tokens functions.
  - Owner can include/exclude from taxes.
  - Owner can withdraw contract tokens.
  - Owner can include addresses in taxExclusionEnabled.

- **XCoffin:**
  - Owner can initialize contract.
  - Owner can take snapshot.
  - Owner can claim community reward.
  - Owner can change communityRewardController address.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details are NOT provided by the team.

TechRate note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.