



ETHOS
AUDIT

Coffee Beans

Audit Report

Apr. 25, 2022

Contents

Executive Summary	3
Audit Details	3
Methodology	3
Contract Details.....	4
Result Summary.....	4
Issues Reported	5
Issues Summary	5
Detailed Findings	5
Code Documentation	5
Adherence to Specifications.....	5
Adherence to Best Practices.....	5
CB-0 – Centralization of referrals	6

Executive Summary

Audit Details

Project Name	Coffee Beans
Codebase	https://bscscan.com/address/0x61654f090f5eb0e851047403b6689d356a9ba09d#code
Initial Audit Date	April 25, 2022
Revision Dates	-
Methodology	Manual

Methodology

This audit's objectives are to evaluate:

- Security-related issues
- Code quality
- Relevant documentation
- Adherence to specifications
- Adherence to best practices

This audit examines the possibility of issues existing along the following vectors (but not limited to):

- Single & Cross-Function Reentrancy
- Front Running (Transaction Order Dependence)
- Timestamp dependence
- Integer Overflow and Underflow
- Mishandled exceptions and call stack limits
- Unsafe external calls
- Number rounding errors
- DoS with (Unexpected) Revert
- DoS with Block Gas Limit
- Insufficient gas grieving
- Forcibly sending native currency
- Logical oversights
- Access control
- Centralization of power
- Logic-Specification Contradiction
- Functionality duplication
- Malicious token minting

The code review conducted for this audit follows the following structure:

1. Review of specifications, documentation to assess smart contract functionality
2. Manual, line-by-line review of code
3. Code's adherence to functionality as presented by documentation
4. Automated tool-driven review of smart contract functionality
5. Assess adherence to best practices
6. Provide actionable recommendations

Contract Details

Contract ID	0x61654F090F5eb0E851047403b6689d356a9Ba09d
Network	BSC
Language	Solidity
Compiler	v0.8.11+commit.d7f03943
Verification Date	Apr. 26, 2022
Libraries	Custom

Result Summary

Ethos' audit of the Coffee Beans smart contract has concluded with a **PASSING** result, meaning the contract is largely safe from external threats but users funds are at the mercy of the team's decision related to the significant referral bonuses collected by the marketing wallet. The initial review identified a number of informational issues, and 2 medium-risk issues, most of which have since been resolved except for the ones reported below. The remaining report includes all issues identified in the initial review, as well as the revised status post resolution by the team if applicable.

- The smart contract is a variant of the 'miner' meta, but a fork of the typical miner codebase
- It allows users to deposit network native tokens into the contract which are locked on deposit and redistributed to users over time
- The rate of redistributions approximately **8% daily** and varies based on the rate of increase of total value locked
- There is a referral bonus distributed to referrers of approximately **12.5%**
- The marketing wallet does accumulate all the referrals where one is not explicitly provided, causing risk of centralization of referral bonuses due to **an additional 12.5% deposit fee taken for marketing**
- There is a **3% dev fee** and a **3% marketing fee** applied on all deposits and withdrawals, and **an additional 12.5% marketing fee** only on deposits made without a referral link
- The contract cannot be closed or shut off at any point after deployment
- While there were a couple of medium-risk issues present in the contract, the Coffee Beans team decided to leave them unresolved or be transparent to users

To conclude, this smart contract does what it is designed to. However, since the marketing wallet accumulates a significant amount of referral bonuses, it can potentially drain the contract over time.

Issues Reported

Severity	Unresolved	Acknowledged	Resolved
Extreme	0	0	0
High	0	0	0
Medium	1	0	0
Low	0	0	0

Issues Summary

ID	Title	Severity	Status
CB-0	Centralization of referrals	Medium	Unresolved

Detailed Findings

Code Documentation

The code has a minimal amount of comments. This could be improved in order to help others understand the contract.

Adherence to Specifications

The smart contract does not adhere to the smart contract functionality described by the Coffee Beans documentation and is not in line with its intended usage. By deciding to leave referral bonuses accruing in the marketing wallet or being transparent with its community about it, they have chosen to take on unnecessary trust from their community and users that the marketing wallet will not cash in the significant amount of accrued referrals.

Adherence to Best Practices

The smart contract adheres to the majority of best practices associated with a standard EVM compatible Solidity smart contract.

CB-0 – Centralization of referrals

Severity: Medium

Status: Unresolved

Description: In the “replant” function, the conditional statement:

```
if (ref == msg.sender | | ref == address(0) | | ref == address(this)) ref = marketingFeeReceiver;
```

makes the referrer of any deposits that do not provide a referrer to default to the marketingFeeReceiver address.

Risk: This allows the marketingFeeReceiver address to accumulate 12.5% referral bonuses from every user that doesn't explicitly use a referral link. There is the potential for the marketing fee wallet to then withdraw these accrued referral bonuses from the contract, which at 12.5% per deposit can be quite significant.

Recommendation: We recommend either redeploying the contract with this line augmented as *if (ref == msg.sender | | ref == address(this)) ref = address(0);*

Alternatively, the team can make be transparent with the community about this feature and just ensure that the ability to take out these referral bonuses are never exercised.

Team comments: The CoffeeBeans team has chosen to leave this issue unresolved and failed to mitigate the risks associated with this issue for the users of the platform by not being transparent about adapting this issue as a feature of the project.