Ethera Black

Smart Contract Security Audit

Date 28/November/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 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 ApeAudits and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (ApeAudits) owe no duty of care towards you or any other person, nor does ApeAudits 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 ApeAudits 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, ApeAudits hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against ApeAudits, 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.

Purpose

This document details ApeAudits' findings and recommended solutions. This audit was performed on November 28, 2021. We did audit a deployed contract. We will update our report if anything changes after launch.

Findings

Token Name	Ethera Black
Token Symbol	ETB

NO.	Audit Items	Audit Subclass	Audit Subclass Result
1	Overflow Audit	N/A	Passed
2	Race Conditions Audit	N/A	Passed
3	Authority Control Audit	Permission Vulnerability Audit Excessive Auditing Authority	Failed Passed
4	Safe Design Audit	Zeppelin Module Safe Compiler Version Hard-coded Version Fallback Function Safeuse Show Coding Security Function Return Value Security Call Function Security	Passed Passed Passed Passed Passed Passed Passed
5	Denial of Service Audit	N/A	Passed
6	Gas Optimization Audit	N/A	Passed
7	Design Logic Audit	N/A	Passed
8	Malicious Event Log Audit	N/A	Passed
9	"False Deposit" Vulnerability Audit	N/A	Passed
10	Uninitialized Storage Pointers Audit	N/A	Passed
11	Arithmetic Accuracy Deviation Audit	N/A	Passed

High Severity Issues

- None.

Medium Severity Issues

- - **Issue:**
  The functions lock(uint256)and unlock()can be used to reclaim ownership after it has been renounced.
  Recommendation:
  Remove the functions or fix the bug.

- - **Issue:**
  Inside the function _transfer(address, address, uint256), in the lines 754 to 794, not all cases are covered. Transfers to addresses that are not the Pancakeswap pair will not incur the default tax fee, but instead will incur the tax fee from the previous transaction. Also, transfers to accounts that are excluded from fees will reset the fees to their state before the previous call to removeAllFee().
  Recommendation:
  Cover the missing cases, and restore the default fees after all transactions.

- - **Issue:**
  The function changeRouterVersion(address) can be used to transfer the fee collection to a different router/pair contract, which could be used maliciously. However, it could also be used to update the contract in case of a Pancakeswap upgrade.
  Recommendation:
  If the contract owner intends to use this functionality, we recommend protecting the owner account carefully, possibly with a multisig wallet. If this is the case, we also recommend fixing the ownership reclaim bug and locking the contract.

- - **Issue:**
  The owner has many other privileges that users should be aware of, such as taking all BNB collected from fees, and setting per-user fees.
  Recommendation:
  If the owner intends to use these features, we recommend being transparent about their reasons. If not, we recommend removing them.

- Low Severity Issues

- **Issue:**
The contract does not add liquidity, unlike its predecessors, and this is not readily apparent information. Functions and events reference adding liquidity, which is misleading. Also, the function `addLiquidity(uint256, uint256)`is never used. Instead, the contract uses collected fees to buy back and burn tokens.

Recommendation:

Rename the incorrectly named functions and events.

Conclusion

Four medium severity issues and one low severity issue found. Contract ownership can be reclaimed through a bug, some unintended fee behaviour when transferring to addresses that are not the Pancakeswap pair, and the owner has a lot of control over the amount of fees collected and their destination. The owner can take all collected fees as BNB and set per-user fees.

ApeAudits note:
Please check the disclaimer above and note, the audit is provided ‘as-is’ and makes no statements or warranties whatsoever. The report is provided only for the contract(s) mentioned in the report.

Appendix

All additional information from our audit can be found at

https://github.com/ApeAudits1/ethera-extras