CoinTool
BlockChain Security

SafeClassic

smart contracts final audit report

Tue Aug 23 2022

cointool.App
cointools@outlook.com

Contents

1. Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice 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.

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

2. Overview

This audit report was generated for SafeClassic with CoinTool token constructor.
The purpose of this audit was to achieve the following:
Identify potential security issues with smart contracts.
Formally check the logic behind given smart contracts.
Information in this report should be used to understand the risk exposure of smart contracts, and as a guide to improving the security posture of smart contracts by remediating the issues that were identified.

We hereby verify that the generated token has identical bytecode with the original audited token.

2.1 Summary

Project Name	SafeClassic
Platform	Ethereum Classic
Language	Solidity
Token	0xEce01807F7d9B93529174533E997e5DE168B0b39

3. List of Audit issues

- logic overview
- Functionality checks
- Following best practices
- Access control and authorization
- Reentrancy attacks
- Front-run attacks
- DoS with (unexpected) revert
- DoS with block gas limit
- Transaction-ordering dependence
- ERC/BEP and other standards violation
- Unchecked math
- Implicit visibility levels
- Excessive gas usage
- Timestamp dependence
- Forcibly sending ether to a contract
- Weak sources of randomness
- Shadowing state variables
- Usage of deprecated code

4. Conclusion

No high severity issues were found.

The audited code is deployed at 0xEce01807F7d9B93529174533E997e5DE168B0b39 in Ethereum Classic (ETC).

Audit includes recommendations on the code improving and preventing potential attacks.

CoinTool.App

BlockChain Security