STRIKEFORCE TECHNOLOGIES

SMART CONTRACT AUDIT REPORT

Fat Cat Killer

By: StrikeForce Technologies, Inc.

Table of Contents

Disclaimer

The report is based on our examination of cybersecurity vulnerabilities of the smart contracts. Strikeforce Technologies disclaims all responsibility and no claim against StrikeForce Technologies can be made to any amount or type of loss or damages (without limitation, direct, indirect, special, punitive, consequential or pure economic loses or losses) that may be caused by any person, or any damages or damages, including without limitations (whether innocent or negligent).

Security analysis is based only on the smart contracts. No applications or operations were reviewed for security. No product code has been reviewed.

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can't guarantee explicit security of the audited smart contracts.

The audit does not give any warranties on the security of the code. One audit cannot beconsidered enough. We always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of the code. Besides a security audit, please don't consider this report as investment advice.

Introduction

This audit report highlights the overall security of the Fat Cat Killer(www.fatcatkiller.com) smart contracts. We have tried to ensure the reliability of the smart contracts by completing the assessment of the smart contract codebase.

In this audit, we consider the following features -

- Whether the code is secure.
- Whether the code meets the best coding practices.

The audit has been performed according to the following procedure:

Manual audit

1. Inspecting the code.
2. Analyzing the code for security vulnerabilities.
3. Assessing the overall project structure, complexity & quality.

Automated analysis was performed using the following tools

1. Mythril
2. Slither
3. Securify2
4. MythX

Audit details

Overview

Website: https://fatcatkiller.com/

Repository Name: fckcoin-contract

Token symbol: $killer

Deployed Address: N/A

Language: Solidity version 0.8.0

Contracts Audited

fckcoin-contract/contracts/

- Control
    - FCKController.sol
    - IFCKController.sol
- foundations
    - FCKFoundation.sol
- governance
    - IVoting.sol
    - Voting.sol
- strategies
    - ITokenomicsStrategy.sol
    - ManualTokenomicsStrategy.sol
- token
    - ERC20.sol
    - FCKToken.sol
    - IFCKToken.sol
- wallets
    - IDistributionWallet.sol

- IOperationalWallet.sol
- IPlatformReserveWallet.sol
- ITokenomicsWallet.sol
- LockupWallet.sol
- MarketingReserveWallet.sol
- OperationalWallet.sol
- PlatformReserveWallet.sol
- TeamAndAdvisorsWallet.sol
- TokenomicsWallet.sol

Audit Findings

Vulnerability	Status
SWC-112 (DELEGATECALL to Untrusted Callee)	No issue detected
SWC-120 (Weak Randomness)	No issue detected
SWC-116 (Timestamp Dependence)	No issue detected
SWC-111 (Use of Deprecated Functions)	No issue detected
SWC-105 (Unprotected Ether Withdrawal)	No issue detected
SWC-110 (Assert Violation)	No issue detected
SWC-117 (Signature Malleability)	No issue detected
SWC-101 (Integer Overflow and Underflow)	No issue detected
SWC-113 (Denial of Service with Failed Call)	No issue detected
SWC-106 (Unprotected SELFDESTRUCT)	No issue detected

SWC-107 (Reentrancy)	No issue detected
SWC-104 (Unchecked Call Return Value)	No issue detected
SWC-110 (Assert Violation)	No issue detected
SWC-124 (Write to Arbitrary Storage Location)	No issue detected
SWC-127 (Arbitrary Jump with Function Type Variable)	No issue detected
SWC-108 (StateVariablesDefaultVisibility)	No issue detected
SWC-109 (Unused Local)	No issue detected
SWC-132 (Incorrect Equality)	No issue detected
SWC-130 (RightToLeftOverride)	No issue detected
SWC-119 (ShadowedStateVariable)	No issue detected

Summary

We tested the smart contracts using multiple tools with varying methodologies. No issues were detected