Audit Whale

Smart contract code review and security analysis report

This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.

The report containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed — upon a decision of the Customer.

Document

Name	Smart Contract Code Review and Security Analysis Report for Smart Harvest.
Approved by	Jameson | COO AuditWhale
Type	---
Platform	All Chains
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Repository	---
Commit	---
Technical Documentation	NO
JS tests	NO
Website	Killking.io
Timeline	05 JANUARY 2022– 12 JANUARY 2022
Change log	18 JANUARY 2022 – INITIAL AUDIT

Table of contents

Introduction

AuditWhale(Consultant) was contracted by Killking (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of the Customer's smart contract and its code review conducted between 05 JANUARY 2022– 12 JANUARY 2022.

Scope

The scope of the project is smart contracts in the repository:
Here are some of the commonly known vulnerabilities that are considered:

Category	Check Item
Code review	▪ Reentrancy ▪ Ownership Takeover ▪ Timestamp Dependence ▪ Gas Limit and Loops ▪ DoS with (Unexpected) Throw ▪ DoS with Block Gas Limit ▪ Transaction-Ordering Dependence ▪ Style guide violation ▪ Costly Loop ▪ Unchecked external call ▪ Unchecked math ▪ Unsafe type inference ▪ Implicit visibility level ▪ Deployment Consistency ▪ Repository Consistency ▪ Data Consistency

Functional review	▪ Business Logics Review ▪ Functionality Checks ▪ Access Control & Authorization ▪ Escrow manipulation ▪ Token Supply manipulation ▪ Assets integrity ▪ User Balances manipulation ▪ Data Consistency manipulation ▪ Kill-Switch Mechanism ▪ Operation Trails & Event Generation

Executive Summary

According to the assessment, the Customer's smart contracts are well-secured.

Our team performed an analysis of code functionality, manual audit, and automated checks with Jameson. All issues found during automated analysis were manually reviewed, and important vulnerabilities are presented in the Audit overview section. All found issues can be found in the Audit overview section.

As a result of the audit, security engineers found 1 low severity issue.

Project	Contract Address	Project Address	Network	Minimum play with
BNB	0xdE54955A453b4Ceb624DA426000d801BAa0EDBAb	0xdE54955A453b4Ceb624DA426000d801BAa0EDBAb	BSC	0.05
AVAX	0xf03188848770C394016D480bDF0b79ed9b5A3126	0xf03188848770C394016D480bDF0b79ed9b5A3126	AVAX	0.7
MATIC	0x19C41FdD878076DE2C6dB78D977e50EAb6364520	0x19C41FdD878076DE2C6dB78D977e50EAb6364520	MATIC	23
CAKE	0x995c745cCd91044625b9563e5947A78E5F68824C	0x995c745cCd91044625b9563e5947A78E5F68824C	BSC	5
BUSD	0x402CEF885875FDF95122C23745cc341d8C1D6e41	0x402CEF885875FDF95122C23745cc341d8C1D6e41	BSC	50
ADA	0x3C9Ed12B513b83393706d9833a0d989d7eb36E8d	0x3C9Ed12B513b83393706d9833a0d989d7eb36E8d	BSC	33
DOGE	0x32dbB9314020783a656CCad3FC750DE2F7A24Aba	0x32dbB9314020783a656CCad3FC750DE2F7A24Aba	BSC	300
LTC	0x0631A8C7e71DB7c1651F2dACee8B9fCfd321a5E9	0x0631A8C7e71DB7c1651F2dACee8B9fCfd321a5E9	BSC	0.039
DOT	0x405ba5a03Dd363b4336357e7031b13a35a452610	0x405ba5a03Dd363b4336357e7031b13a35a452610	BSC	2
XRP	0xfb7A0fF802F3c5d9dc4857d31D0cf92644010464	0xfb7A0fF802F3c5d9dc4857d31D0cf92644010464	BSC	66
BTCB	0x508385fB305022b27D9C90Cbc872B3109C18116a	0x508385fB305022b27D9C90Cbc872B3109C18116a	BSC	0.0012
SAFEMOON	0x4fF9B5b7703108b5749aC0e32C1E65aa5582aA2A	0x4fF9B5b7703108b5749aC0e32C1E65aa5582aA2A	BSC	29404122
TT	0x8F87E9858c22c3Ac63526d1B0C1bbB37A7FAa870	0x8F87E9858c22c3Ac63526d1B0C1bbB37A7FAa870	Thundercore	1264.01157

On chain Games:

Games	Winner ratio	Probability
Kill King	200%,180%,150%,120%,100%,50%	60%
King Pool	200%,180%,150%,120%,100%,50%	80%

Referral System (Match Bonus):

- No referral system implemented

Withdraw:

- No user request implemented.
- winning amount will be instantly.

.

Audit overview & Severity Definitions:

CRITICAL ISSUES (critical,high severity):	0
HIGH ISSUES (high, medium severity):	1
ERRORS, WARNINGS (medium, low severity):	0
OPTIMIZATION (low severity):	1
RECOMMENDATIONS (very low severity):	0

High ISSUE:

The system implemented is completely on a random number based system, which matches on the user deposit instance

User's play amount is not limited to higher level but a minimum of 50$(approx) was implemented in all the contracts. Noguaranteeofcompulsorywin. Winning bonus are paid instantly as internal transaction of the deposit transactions. Do always invest with proper knowledge andinvestigation.

Optimization suggestions:

Loop on the dynamic variable (low severity).

If the user gets more parallel deposits his withdrawal transaction going to cost more transaction fee because the loop on the dynamic variable is used in the 'withdraw' function.

Caution:

In case exceeding the GAS limit of the size of the transaction game play is not possible.

Note:

This comment is relevant only if a user creates an excessive amount of parallel users playing with the game .

Independent description of the smart-contract functionality:

The smart contract is a gaming contract which allows users to bet and win/lose amount randomly and get a profits upto 200% on the investment and a chance of losing them as well.

Kill king pool is a queue process of investment where you get a chance of winning upto 200%of investment after the completion of the stack user count . All the returns are completely depends on the deposits in the pool and the time period that is taken to complete the pool time.

Conclusion

In the Kill-King Smart-Contract were found no vulnerabilities, no backdoors, and no scam scripts.

The code was tested with compatible compilers and simulated manually reviewed for all commonly known and specific vulnerabilities.

So Kill-King Smart-Contract is safe for use in the All Chain main networks.

Disclaimers

This audit is only to the Smart-Contract code at the specified address.

Audit Whale is a 3rd party auditing company that works on audits based on client requests. And as a professional auditing firm, we check on the contract for any vulnerabilities, backdoors, and/or scam scripts.

Therefore:

We are not financial advisors nor do we partner with the contract owners

Operations and website administration is fully on the client's side

We do not have influence over client operations, which can lead to website changes, withdrawal function closes, etc. One always has the option to do this through the contract.

Any concerns about the project themselves need to be raised directly to the project owners and not through Audit Whale.

Investors are not in any way obliged, coerced or influenced to invest in projects audited by Audit Whale.

We are not responsible for your funds or guarantee you profits.

We highly recommend that investors do their own research and gain crypto experience before investing