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	Smartharvest.io
Timeline	28 DECEMBER 2021 – 02 JANUARY 2022
Change log	02 JANUARY 2022 – INITIAL AUDIT

Table of contents

Introduction	4
Scope	4
Executive Summary	5
Severity Definitions	5
Audit overview	7
Conclusion	7
Disclaimers	9

Introduction

AuditWhale(Consultant) was contracted by SmartHarvest (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 December 28th, 2021 - JANUARY 02nd, 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	Min Deposit
LTC	0xe271E64EA234ABECc95E9d011d8082B49622A35F	0xe271E64EA234ABECc95E9d011d8082B49622A35F	BSC	0.35
AVAX	0x28350e8950DCC08337EFef6780CdA42D46027Cde	0x28350e8950DCC08337EFef6780CdA42D46027Cde	BSC	0.5
CAKE	0x75d80ec47330d078368a064033DC273792146034	0x75d80ec47330d078368a064033DC273792146034	BSC	5
BUSD	0x455276b87D33ee6Eb406DEfC59C8A43735D5993E	0x455276b87D33ee6Eb406DEfC59C8A43735D5993E	BSC	50
DOGE	0x9AEB96521D7ebB57Cd6872Cdc943aB89DF983889	0x9AEB96521D7ebB57Cd6872Cdc943aB89DF983889	BSC	300
DOT	0xc4CC436226026Ca46b33B33848D92458e0b213f2	0xc4CC436226026Ca46b33B33848D92458e0b213f2	BSC	1.7
XRP	0xEbEd408192A4237b1dC1126535b7f0f0A5Bc3e15	0xEbEd408192A4237b1dC1126535b7f0f0A5Bc3e15	BSC	61
BTCB	0x8f61FC690742d540864dfA6a48877aa5253E52cc	0x8f61FC690742d540864dfA6a48877aa5253E52cc	BSC	0.0011
BNB	0xEf2A1A8Ee8F1Ef5D1698caa68Bfd06CedA834231	0xEf2A1A8Ee8F1Ef5D1698caa68Bfd06CedA834231	BSC	0.1
MATIC	0xf1f14A0fFF6AaBD137d937bCB149379aB2607EDA	0xf1f14A0fFF6AaBD137d937bCB149379aB2607EDA	POLYGON	0.2
TRX	TNpiyM5pxyTcKnPkUZiD2JWnKBYaoRcLaE	TNpiyM5pxyTcKnPkUZiD2JWnKBYaoRcLaE	TRON	1200
SAFEMOON	0xc3Fb7506DAace8f2C286628Fd8f7F10259E3878c	0xc3Fb7506DAace8f2C286628Fd8f7F10259E3878c	BSC	19000
USDT	TSKrAwzTUMXinfn3BiUznv6oS6q65tcC73	TSKrAwzTUMXinfn3BiUznv6oS6q65tcC73	TRON	50
ADA	0x846F8650eCb1cBeB7297AfCAbD9C349a366b56F5	0x846F8650eCb1cBeB7297AfCAbD9C349a366b56F5	BSC	38
TT	0x0a1f4de24f242111c5f14477ac65aceabf2b41db	0x0a1f4de24f242111c5f14477ac65aceabf2b41db	Thundercore	6314.510619

Contract Owners Fee:

Invest: **10%**

Plans	Total Returns	Daily Profit	Days
1	200%	5%	40
2	240%	4%	60
3	300%	3%	100

Referral System (Match Bonus):

The contract pays a 12% referral commission over 3 levels

Level 1: 5%
Level 2: 4%
Level 3: 3%

Notes:

- Referral should be an active user; it means the referral address has at least one deposit
- The referrer is specified once at the time of the first deposit and is assigned to the user without the possibility of changing. From each subsequent Deposit, the referrer will get his percent.
- If a user has not had a valid up line, a total referral commission will be sent to the owner

Withdraw:

- Users can withdraw profits any time.
- The capital deposit cannot be withdrawn , user is able to withdraw his yield only .

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 used is called ROI and must be considered as HIGH-RISK.

User's principal deposits cannot be withdrawn, users can get dividends and referral commission. Dividends are paid from deposits of other users. Do always invest with proper knowledge and investigation.

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 withdraw is not possible.

Note:

This comment is relevant only if a user creates an excessive amount of parallel deposits (more than 100).

Independent description of the smart-contract functionality:

The smart contract provides the opportunity to invest any amount in BNB, BUSD, SHIB, and USDT in the contract and get a 200% profit on investment in 40 days if the contract balance has enough funds for payment.

All dividends are calculated at the moment of request and available for withdrawal once a day
Capital investment can be withdrawn at the end of the plan
Each subsequent Deposit is kept separately in the contract, to maintain the payment amount for each Deposit.

Conclusion

In the SmartHarvest 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 SmartHarvest 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