HackSafe

Smart Contract Security Audit Report

Zombiverse

July 2022

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
Zombiverse

Deployer address
0xe364f4d13E22c7858085443406 3F2a7b07e1F594

Client contacts
Zombiverse

Blockchain
Binance Smart Chain

Website
https://zombiverse.app/

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

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by Zombiverse to perform an audit of smart contract:

- https://bscscan.com/address/0xf01895a61a34072415E6376392b89BFBa7958C50#code

The purpose of the audit was to achieve the

- Ensutre that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contract Details

Token contract details for 11.07.2022

Token Type	: BEP20
Contract name	: Zombiverse
Contract address	: 0xf01895a61a34072415E6376392b89BFBa7958C50
Compiler version	: v0.8.15+commit.e14f2714
Total supply	: 20,000,000,000
Token Ticker	: ZBV
Decimals	: 18
Token Holders	: 1,175
Top 100 token holder's dominance	: 98.06%
Transactions count	: 3,960
Contract deployer address	: 0xe364f4d13E22c7858054344063F2a7b07e1F594
Owner address	: 0x0000000000000000000000000000000000000000
Burner address	: 0x569FF8eDdd91A93F12d48e1CbD4906De342772D1

Social profiles

Twitter Profile	: https://twitter.com/zombiebsc
Telegram Profile	: https://t.me/zbvgroup
Coinmarketcap profile	: https://coinmarketcap.com/currencies/zombiverse/

Claimed Smart Contract Features

Claimed Feature Detail

Tokenomics :

- **Name** : ZombiVerse
- **Symbol** : ZBV
- **Decimals** : 9
- **Protocol** : BEP20
- **Total supply** : 20,000,000,000
- **Contract address** : 0x4a846D300F793752eE8bd579192C477130C4B369

Our Observation

YES, this is valid, but Whitepaper explain to have the 9 decimals in contract but deployed contract has 18 decimals.

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are “Secure”. This token contract does contain owner control, which do not make it fully decentralized as owner does have control over smart contract.

Insecure	Poor secured	Secure	Well-secured

You are here 

We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 0 medium and 1 low and some very low-level issues. These issues are not critical ones.

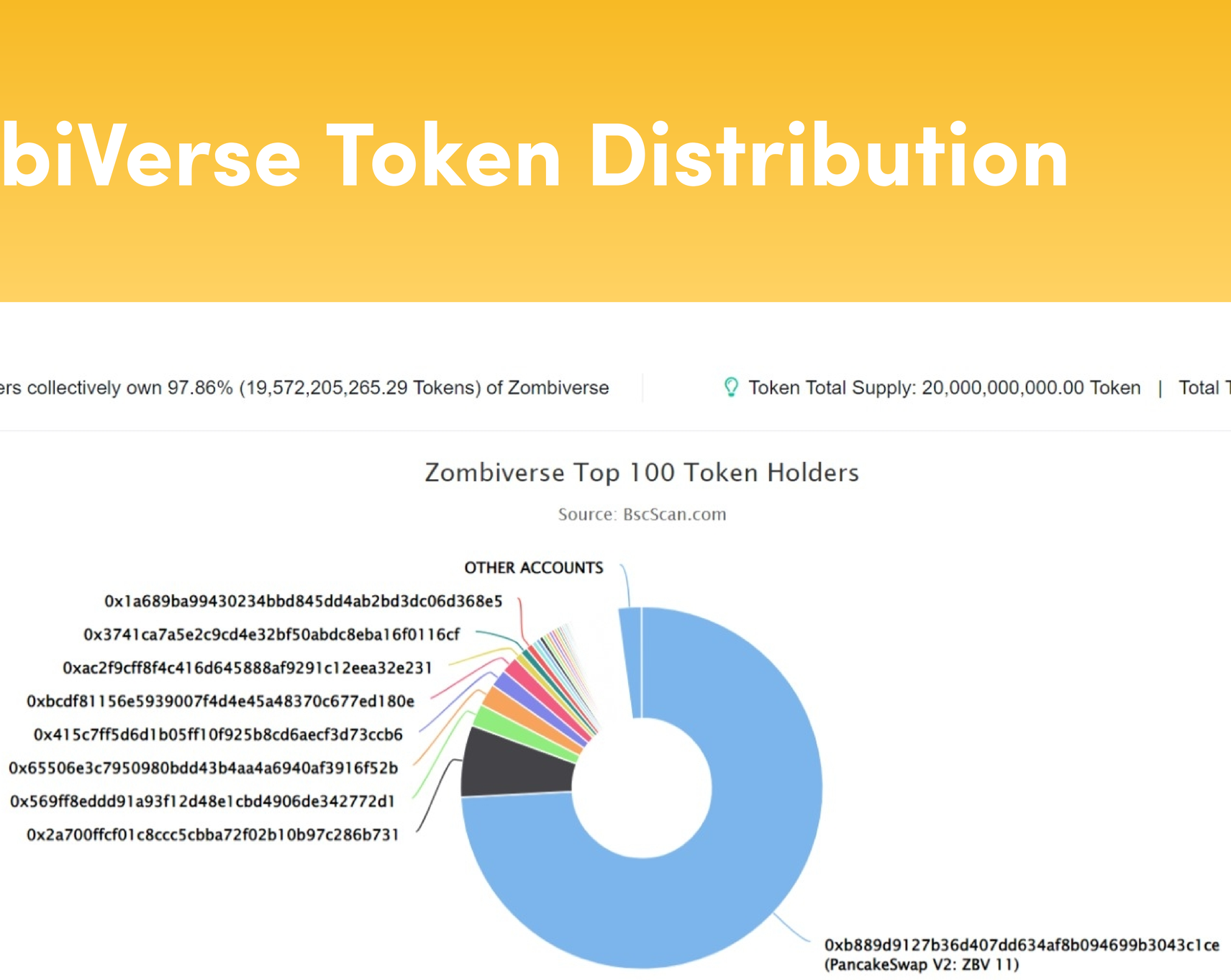
ZombiVerse Token Distribution

The top 100 holders collectively own 97.86% (19,572,205,265.29 Tokens) of Zombiverse

Token Total Supply: 20,000,000,000.00 Token | Total Token Holders: 1,182

Zombiverse Top 100 Token Holders

Source: BscScan.com



Zombiverse Token Top 20 Token Holders

(A total of 19,572,205,265.29 tokens held by the top 100 accounts from the total supply of 20,000,000,000.00 token)

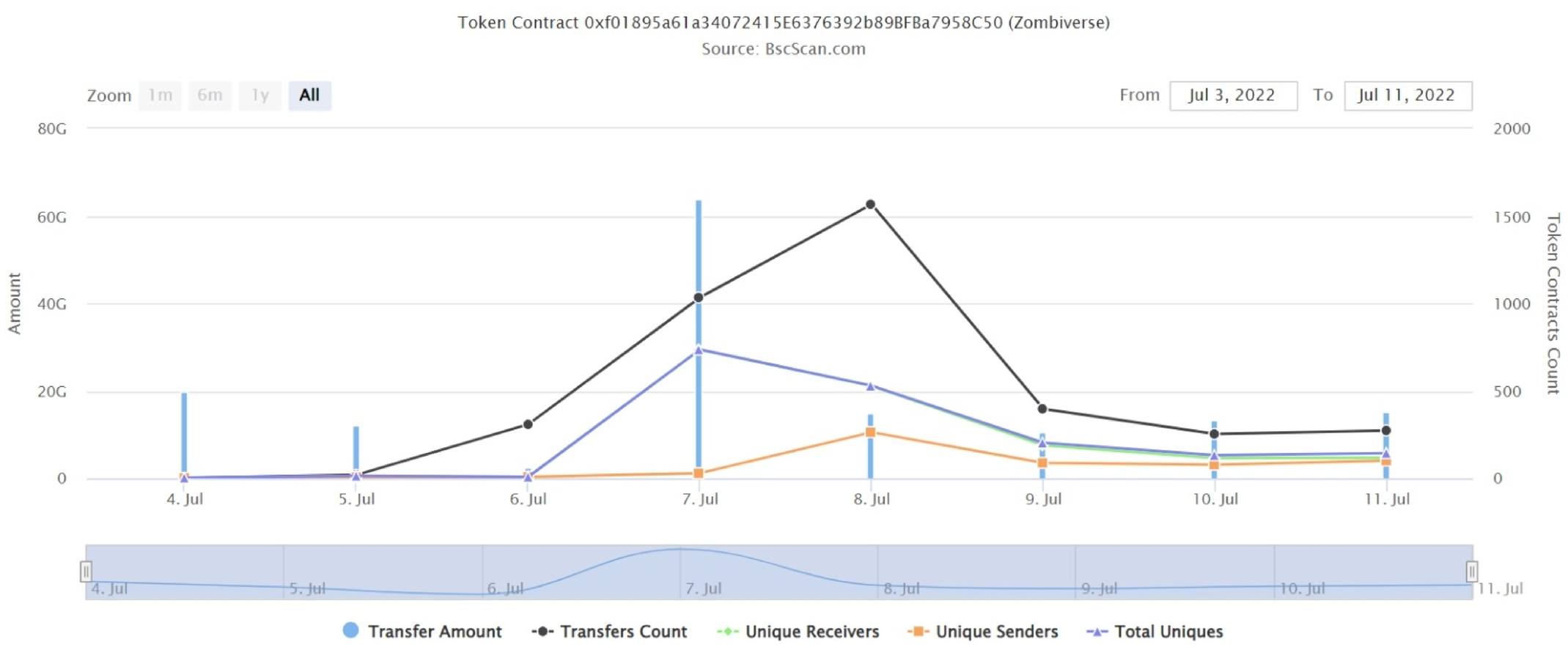
Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap V2: ZBV 11	14,835,514,671.317468175039054973	74.1776%
2	0x2a700ffcf01c8ccc5cbba72f02b10b97c286b731	1,289,771,114.033213107574136747	6.4489%
3	0x569ff8eddd91a93f12d48e1cbd4906de342772d1	400,000,000	2.0000%
4	0x65506e3c7950980bdd43b4aa4a6940af3916f52b	399,338,000	1.9967%
5	0x415c7ff5d6d1b05ff10f925b8cd6aecf3d73ccb6	313,296,846.068511550603537341	1.5665%
6	0xbcdf81156e5939007f4d4e45a48370c677ed180e	300,000,000	1.5000%
7	0xac2f9cff8f4c416d645888af9291c12eea32e231	136,598,184.150856210724740001	0.6830%
8	0x3741ca7a5e2c9cd4e32bf50abdc8eba16f0116cf	129,669,084.824840568913979679	0.6483%
9	0x1a689ba99430234bbd845dd4ab2bd3dc06d368e5	121,857,080.826359272231637824	0.6093%
10	0x9ee627c76ee63484717101e660afd3529c5aa313	85,628,106.105214477463964697	0.4281%
11	0x9044030376f521794ad1481779d78dbab63df106	74,396,265.205034187344591138	0.3720%
12	0xd66fb5c3a395f915f2cbb59dbe59c42114d3de9d	69,782,705.10561599156277476	0.3489%
13	0x42f8dccff318f1870c6e28f2f777705b11288040	60,853,614.85388654695001376	0.3043%
14	0xcf99be7cab8952e2a58e0d0ad24a3dd33d0972c4	59,317,340.555080108087029424	0.2966%
15	0x608f051f07ef8a9be80a1aa4b0caf591a1c62c4f	59,176,829.561811626163422976	0.2959%
16	0xaffcbcaeb215668a345672fa498115c0fb705fe2	53,646,654.871413209842595757	0.2682%
17	0x2bb78f53a6972546ce42376d6dafd29329966057	52,796,512.793362883264125759	0.2640%
18	0xb6429ce6ab1089b1ef66a871c924ee088138b0ff	44,661,630.445410049145818093	0.2233%
19	0x0a9a5245da8653b99f2af3dbf03054dec3ff024e	42,410,139.112039670393617196	0.2121%
20	0x5c1ed844477e4e21708b37d3c777ca70364da46b	39,988,533.578601264650008657	0.1999%

ZombiVerse Token Distribution

ZombiVerse Token Contract Overview

Time Series: Token Contract Overview

Mon 4, Jul 2022 - Mon 11, Jul 2022



Contract functions details

+ [Int] IERC20
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] transfer
    -[Ext] allowance
    -[Ext] approve
    -[Ext] transferFrom

+[Int] IERC20Metadata (IERC20)
    -[Ext] name
    -[Ext] symbol
    -[Ext] decimals
+ Context
    -[Int] _msgSender
    -[Int] _msgData
+ Ownable (Context)
    -<constructor>
    -[Pub] owner
    -[Pub] renounceOwnership #
      -modifiers: onlyOwner
    -[Pub] transferOwnership
      -modifiers: onlyOwner
    -[Int] _setOwner

+ Zombiverse(Context, IERC20, IERC20Metadata,Ownable)
    - < constructor>
    - [Pub] burn #
      - modifiers: onlyDev
    - [Pub] updateBurner #
      -modifiers: onlyDev
    - [Pub] withdrwal #
      -modifiers: onlyDev
    - [Ext] node
    -[Pub] name
    -[Pub] symbol
    -[Pub] decimals
    -[Pub] totalSupply
    -[Pub] burner #

Contract functions details

-[Pub] balanceOf
-[Pub] transfer #
-[Pub] allowance
-[Pub] approve #
-[Pub] transferFrom #
-[Pub] increaseAllowance
-[Pub] decreaseAllowance
-[Int] _transfer #
-[Int] _mint#
-[Int] _burn #
-[Int] _approve #
-[Int] _beforeTokenTransfer #
-[Int] _afterTokenTransfer #

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

Critical Severity Issues

No critical severity issue found.

High Severity Issues

No high severity issue found.

Medium Severity Issues

No medium severity issue found.

Low Severity Issues

One low severity issue found..

1. Unlocked Compiler Version.

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version ^0.8.9 the contract should contain the following line:

  pragma solidity 0.8.15;

Centralization

Burner Privileges :

- ZombiVerse Contract:
    - Burner can add new burner address.
    - Burner can withdraw tokens and native coin from smart contract.
    - Burner can add address if it set to true then that user will not be able to transfer amounts.

Owner privileges :

- ZombiVerse Contract:
    - Owner can remove and transfer ownership.

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble but smart contract ownership has been renounced. Following are Admin functions and burner functions:

- Transferownership
- Renounceownership
- Burn
- Updateburner
- Withdrwal

Conclusion

Smart contract contains low severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.