HackSafe

Smart Contract Security Audit Report

Zippie

January 2023

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
Zippie

Deployer address
0x21ef24ffb2116f44e7918a80cea4f52a2ea72b17

Client contacts
Zippie

Blockchain
Ethereum

Website
https://zippie.org/

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 Zippie to perform an audit of smart contracts:

- https://etherscan.io/token/0xedd7c94fd7b4971b916d15067bc454b9e1bad980#code

The purpose of the audit was to achieve the following:

- Ensure 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 10.01.2023

Token Type	: DEFI
Contract name	: ZipToken
Contract address	: 0xEDD7c94FD7B4971b916d15067Bc454b9E1bAD980
Total supply	: 1,000,000,000
Token ticker	: ZIPT
Decimals	: 18
Token Holders	: 2,764
Transactions count	: 25,907
Compiler version	: v0.4.21+commit.dfe3193c
Contract deployer address	: 0x21ef24ffb2116f44e7918a80cea4f52a2ea72b17
Owner address	: 0xEDD7c94FD7B4971b916d15067Bc454b9E1bAD980

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.

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, 1 medium and 1 low.

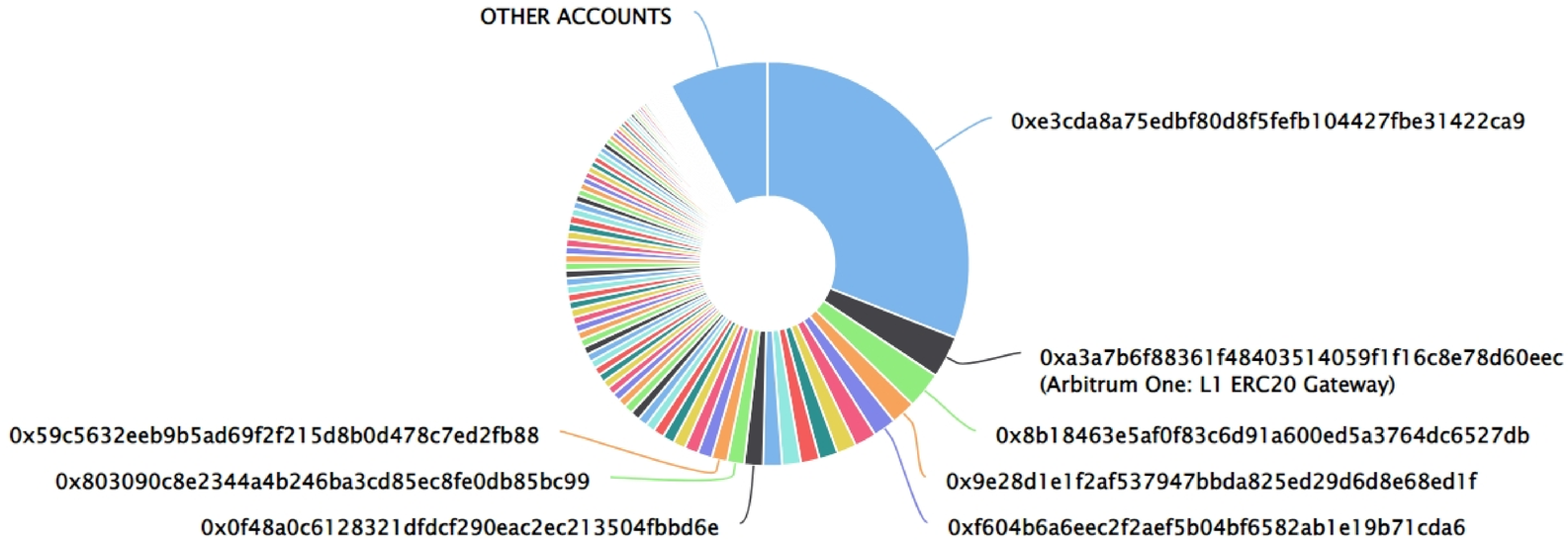
Zippie Token Distribution

The top 100 holders collectively own 92.08% (920,817,708.44 Tokens) of Zippie

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 2,764

Zippie Top 100 Token Holders

Source: Etherscan.io



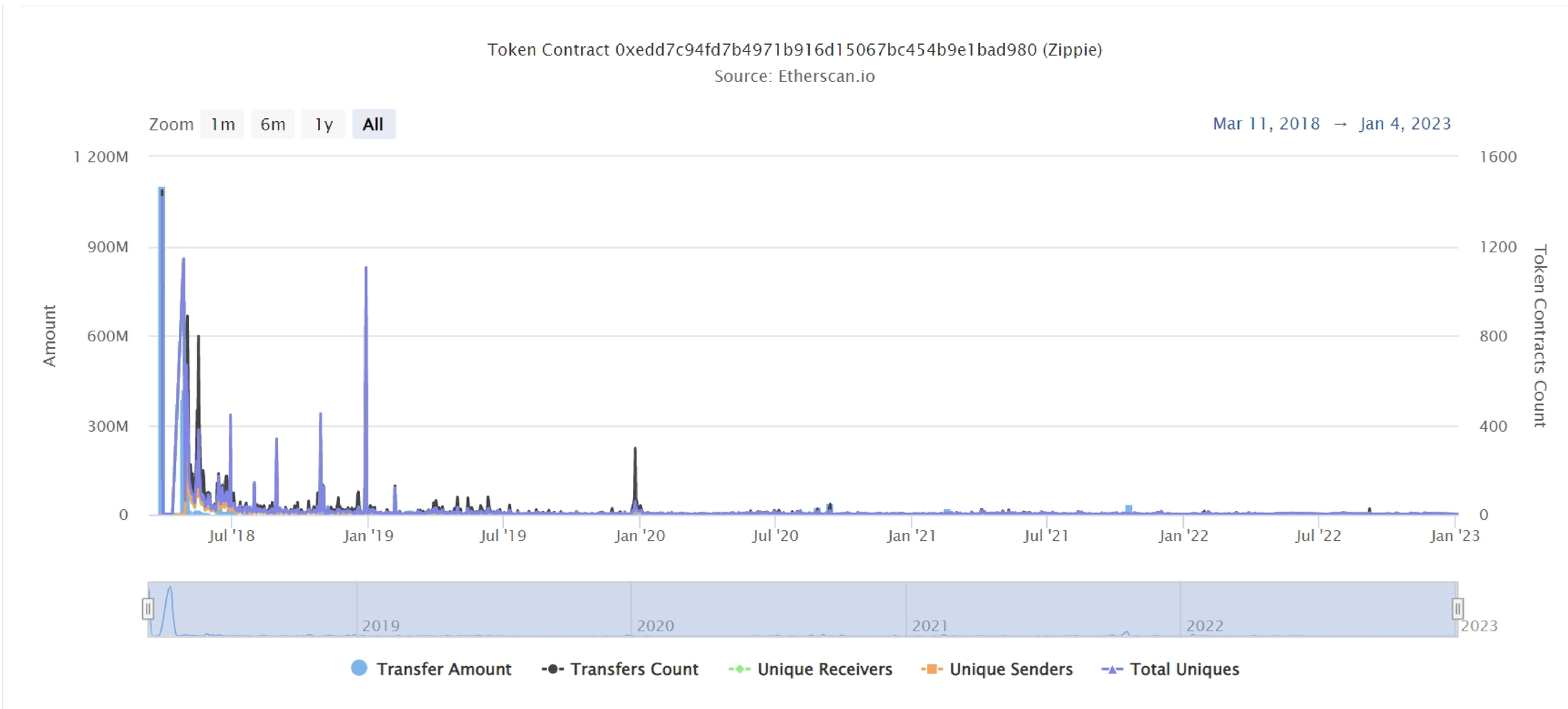
Zippie Top 20 Token Holders

(A total of 920,817,708.44 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xe3cda8a75edbf80d8f5fefb104427fbe31422ca9	310,000,000	31.0000%
2	Arbitrum One: L1 ERC20 Gateway	33,563,922.566934125161571353	3.3564%
3	0x8b18463e5af0f83c6d91a600ed5a3764dc6527db	29,113,482.676854432096278729	2.9113%
4	0x9e28d1e1f2af537947bbda825ed29d6d8e68ed1f	19,749,000	1.9749%
5	0xf604b6a6eec2f2aef5b04bf6582ab1e19b71cda6	18,314,659.99999999	1.8315%
6	0x214933bbaf268cf635369d221e4521face27dbc3	17,426,000	1.7426%
7	0xed2fafbecc86240609d0af0491cd89d6eb21d64c	15,461,000	1.5461%
8	0xb9c36fe4f27164fca364cb855f5a751913cc8e51	15,000,000	1.5000%
9	0xab86e0998fee134ad0d36478ea5f86dbd4d8f4cc	15,000,000	1.5000%
10	0xe691d5a3267eebd4e9fda831237c89a154d00fdc	15,000,000	1.5000%
11	0x1f2cc1f815756e5749689ad2ab8c5a8486b308bf	15,000,000	1.5000%
12	0x0f48a0c6128321dfdcf290eac2ec213504fbbd6e	15,000,000	1.5000%
13	0x803090c8e2344a4b246ba3cd85ec8fe0db85bc99	13,791,000	1.3791%
14	0x59c5632eeb9b5ad69f2f215d8b0d478c7ed2fb88	12,370,000	1.2370%
15	0x2eba521cf8a7c2b10b1ae1ed76ad735bd9206dac	11,400,000	1.1400%
16	0xde1b4b0909bb1e61bcb2d5bf179c4c8d5b88b465	11,155,000	1.1155%
17	0x3042222bb2f9d5510d5264ebdf2d4799d3368583	10,114,000	1.0114%
18	0xa391f0de0b6dac0261c97f47b6dc1f75af68a08a	9,221,000	0.9221%
19	0x459678d89ffb6ead017c4b256990533337696fb6	8,452,000	0.8452%
20	0x649d19f19f509547dac1997bf685a7d799ba95a8	7,790,000	0.7790%

Zippie Token Distribution

Zippie Contract Overview



Contract functions details

+Ownable
  -[Pub] Ownable
  -[Pub] transferOwnership #
    -modifiers: onlyowner

+Pausable (Ownable)
  -[Pub] pause #
    -modifiers: onlyowner, whennotpaused
  -[Pub] unpause #
    -modifiers: onlyowner, whenpaused

+[Lib] SafeMath
  -[Int] mul
  -[Int] div
  -[Int] sub
  -[Int] add

+ERC20Basic
  -[Pub] totalSupply
  -[Pub] balanceOf
  -[Pub] transfer #

++BasicToken (ERC20Basic)
  -[Pub] totalSupply
  -[Pub] transfer #
  -[Pub] balanceof

+ERC20 (ERC20Basic)
  -[Pub] allowance
  -[Pub] transferFrom #
  -[Pub] approve #

+StandardToken (ERC20, BasicToken)
  -[Pub] transferFrom #
  -[Pub] approve #
  -[Pub] allowance
  -[Pub] increaseapproval #
  -[Pub] decreaseapproval #

+PausableToken (StandardToken, Pausable)
  -[Pub] transfer #
    -modifiers: whennotpaused

Contract functions details

-[Pub] transferFrom #
  -modifiers: whennotpaused
-[Pub] approve #
  -modifiers: whennotpaused
-[Pub] increaseApproval #
  -modifiers: whennotpaused
-[Pub] decreaseApproval #
  -modifiers: whennotpaused

+ZipToken (PausableToken)
  -[Pub] ZipToken#
  -[Pub] distributeTokens #
    -modifiers: onlyowner

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Compiler error	Passed
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.	Medium Issue
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	Low issue

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

One medium severity issue found.

1. Out of gas limit

- **Description**

  The function distributeTokens() uses the loop to add transfer tokens. Function will be aborted with OUT_OF_GAS exception if there will be a long length of addresses of array.

- **Recommendation**

  Use EnumerableSet instead of array or do not use long arrays.

Low Severity Issues

One low severity issue found.

1. Old compiler version

- **Description**

  Contract has been deployed using too old solidity version.

- **Recommendation**

  It is advisable to deploy contract using any of the latest version of solidity.

Centralization

Owner privileges :

- Zippie Contract:
    - Owner can transfer tokens to multiple addresses.
    - Owner can pause and unpause transfers.

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, as smart contract ownership has not been renounced. Following are Admin functions:

- Transferownership
- Pause
- Unpause
- Distributetokens

Conclusion

Smart contract contains medium and 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.