HackSafe

Smart Contract Security Audit Report

SQUEEZE

April **2022**

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
SQUEEZE

Deployer address
0x6672C7bb6E698145abA8b2f35CBE20a6901687A9

Client contacts
SQUEEZE team

Blockchain
Ethereum

Website
Not provide by SQUEEZE team.

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.

Background

HeckSafe was commissioned by SQUEEZE to perform an audit of smart contracts:

- https://etherscan.io/address/0xabd4dc8fde9848cbc4ff2c0ee81d4a49f4803da4#code

Contract Details

Token contract details for 16.04.2022

Contract name	: SQUEEZE
Contract address	: 0x76F34cd142ca4a5ea2E197ebffbF5234A1c29268
Total supply	: 100, 000, 000, 000, 000
Token Ticker	:SQUEEZE TOKEN
Decimals	: 9
Token Holders	: 393
Transactions count	: 2,219
Contract deployer address	0x6672C7bb6E698145abA8b2f35CBE20a6901687A9
Owner address	: 0x0000000000000000000000000000000000000000

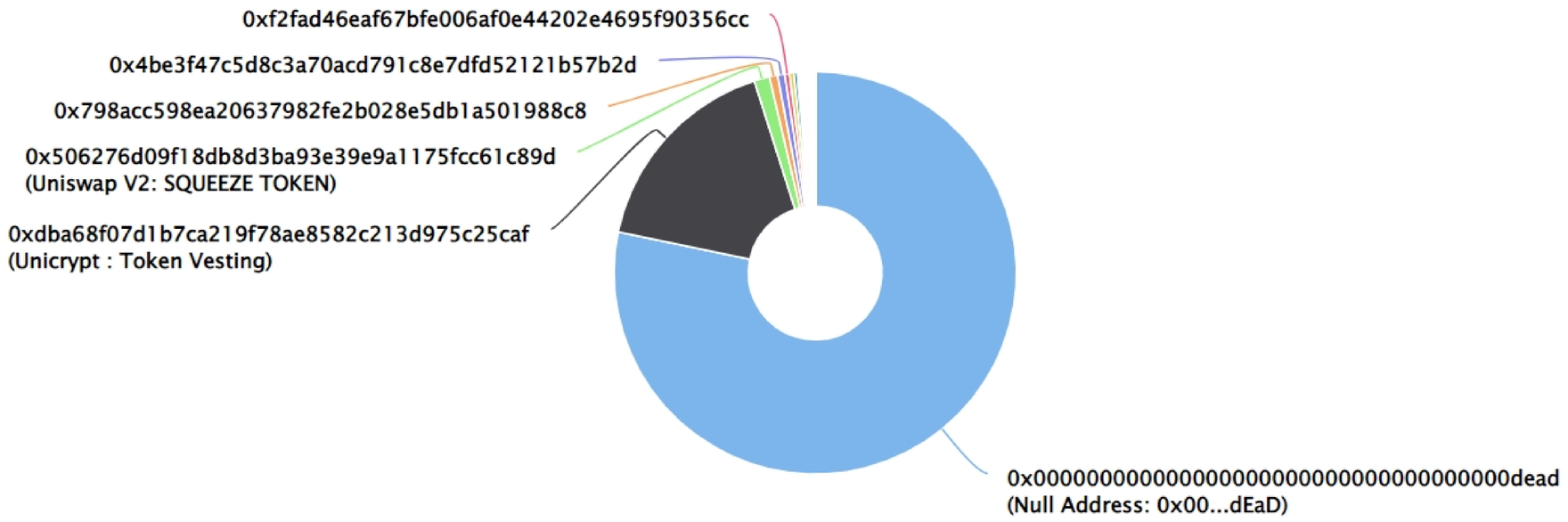
SQUEEZE Token Distribution

The top 500 holders collectively own 100.00% (99,997,019,744,937.70 Tokens) of SQUEEZE

Token Total Supply: 100,000,000,000,000.00 Token | Total Token Holders: 393

SQUEEZE Top 500 Token Holders

Source: Etherscan.io



SQUEEZE Top 10 Token Holders

(A total of 98,811,786,709,332.20 tokens held by the top 10 accounts from the total supply of 100,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x00...dEaD	78,263,830,119,282.276533922	78.2638%
2	Unicrypt : Token Vesting	16,843,473,342,911.99469836	16.8435%
3	Uniswap V2: SQUEEZE TOKEN	1,238,006,448,035.093071607	1.2380%
4	0x798acc598ea20637982fe2b028e5db1a501988c8	661,522,265,299.470238343	0.6615%
5	0x4be3f47c5d8c3a70acd791c8e7dfd52121b57b2d	574,515,307,183.049487634	0.5745%
6	0xf2fad46eaf67bfe006af0e44202e4695f90356cc	369,836,092,314.448575963	0.3698%
7	0x6cec78ff08cd4bbf36e54d4d11ca7882273c9334	363,327,039,490.221952866	0.3633%
8	0xeec7742fe4c2feab750f319c9613b9f168cf4167	268,537,036,180.080969586	0.2685%
9	Hotbit 3	137,988,752,324.03329141	0.1380%
10	0x4ba0e95ffb9b5fb971588c834b18758bbfe8015e	90,750,306,311.503547764	0.0908%

Contract functions details

+ Context
    - [Int] _msgSender

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

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

+ Ownable (Context)
    - < Constructor >#
    - [Pub] owner
    - [Pub] renounceOwnership #
      - modifiers: onlyOwner

+ [Int] IUniswapV2Factory
    - [Ext] createPair #

+ [Int] IUniswapV2Router02
    - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
    - [Ext] factory
    - [Ext] WETH
    - [Ext] addLiquidityETH ($)

+ Squeeze (Context, IERC20, Ownable)
    - <Constructor> #
    - [Pub] name
    - [Pub] symbol

Contract functions details

- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Ext] setCooldownEnabled #
  - modifiers: onlyOwner
- [Pvt] tokenFromReflection
- [Pvt] _approve #
- [Pvt] _transfer #
- [Pvt] swapTokensForEth #
  - modifiers: lockTheSwap
- [Pvt] sendETHToFee #
- [Ext] openSwapTrading #
  - modifiers: onlyOwner
- [Ext] setSwapEnabled #
- [Pub] setBots #
  - modifiers: onlyOwner
- [Pub] delBot #
  - modifiers: onlyOwner
- [Pvt] _tokenTransfer #
- [Pvt] _transferStandard #
- [Pvt] _takeTeam #
- [Pvt] _reflectFee #
- [Ext] ($)
- [Ext] manualswap #
- [Ext] manualsend #
  - [Pvt] _getValues
  - [Pvt] _getTValues
  - [Pvt] _getRValues
  - [Pvt] _getRate
  - [Pvt] _getCurrentSupply

($) = 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

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 issues 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 v0.8.4 the contract should contain the following line:

  pragma solidity 0.8.4;

Owner Privileges

Owner Privileges (in the period when the owner is not renounced) :

- SQUEEZE Contract:
    - Owner can enable cooldown (user to user trading with time offset).
    - Owner can open swap trading.
    - Owner can add and remove bots (no transferring between this addresses).
    - Owner can renounce owner ship.

Conclusion

Smart contract contains low severity issues! liquidity pair contract's security is not checked due to out of scope.

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.