soken

SMART CONTRACT SECURITY AUDIT

Project Vivy

Scan and check this report was posted at Soken Github

May, 2022

Website: soken.io

Table of Contents

Disclaimer

This is a comprehensive report based on our automated and manual examination of cybersecurity vulnerabilities and framework flaws. We took into consideration smart contract based algorithms, as well. Reading the full analysis report is essential to build your understanding of project's security level. It is crucial to take note, though we have done our best to perform this analysis and report, that you should not rely on the our research and cannot claim what it states or how we created it. Before making any judgments, you have to conduct your own independent research. We will discuss this in more depth in the following disclaimer - please read it fully.

DISCLAIMER: You agree to the terms of this disclaimer by reading this report or any portion thereof. Please stop reading this report and remove and delete any copies of this report that you download and/or print if you do not agree to these conditions. This report is for non-reliability information only and does not represent investment advice. No one shall be entitled to depend on the report or its contents, and Soken and its affiliates shall not be held responsible to you or anyone else, nor shall Soken provide any guarantee or representation to any person with regard to the accuracy or integrity of the report. Without any terms, warranties or other conditions other than as set forth in that exclusion and Soken excludes hereby all representations, warrants, conditions and other terms (including, without limitation, guarantees implied by the law of satisfactory quality, fitness for purposes and the use of reasonable care and skills). The report is provided as "as is" and does not contain any terms and conditions. Except as legally banned, Soken disclaims all responsibility and responsibilities and no claim against Soken is made to any amount or type of loss or damages (without limitation, direct, indirect, special, punitive, consequential or pure economic loses or losses) that may be caused by you or any other person, or any damages or damages, including without limitations (whether innocent or negligent).

Security analysis is based only on the smart contracts. No applications or operations were reviewed for security. No product code has been reviewed.

Procedure

Our analysis contains following steps:

1. Project Analysis;

2. Manual analysis of smart contracts:
- Deploying smart contracts on any of the network(Ropsten/Rinkeby) using Remix IDE
- Hashes of all transaction will be recorded
- Behaviour of functions and gas consumption is noted, as well.

3. Unit Testing:
- Smart contract functions will be unit tested on multiple parameters and under multiple conditions to ensure that all paths of functions are functioning as intended.
- In this phase intended behaviour of smart contract is verified.
- In this phase, we would also ensure that smart contract functions are not consuming unnecessary gas.
- Gas limits of functions will be verified in this stage.

4. Automated Testing:
- Mythril
- Oyente
- Manticore
- Solgraph

Terminology

We categorize the finding into 4 categories based on their vulnerability:

- Low-severity issue — less important, must be analyzed
- Medium-severity issue — important, needs to be analyzed and fixed
- High-severity issue —important, might cause vulnerabilities, must be analyzed and fixed
- Critical-severity issue —serious bug causes, must be analyzed and fixed.

Limitations

The security audit of Smart Contract cannot cover all vulnerabilities. Even if no vulnerabilities are detected in the audit, there is no guarantee that future smart contracts are safe. Smart contracts are in most cases safeguarded against specific sorts of attacks. In order to find as many flaws as possible, we carried out a comprehensive smart contract audit. Audit is a document that is not legally binding and guarantees nothing.

Token Contract Details for 03.05.2022

Contract Name: **ProjectVivy**

Deployed address: **0x43c7BF973Dd82e536d8F6EA9562d8Fdf876Ca707**

Total Supply: **1,000,000,000**

Token Tracker: **VIVY**

Decimals: 1**8**

Token holders: **131**

Transactions count: **748**

Top 100 holders dominance: **99.74%**

Audit Details

Project Name: **Project Vivy**

Language: **Solidity**

Compiler Version: **v0.8.13**

Blockchain: **Ethereum**

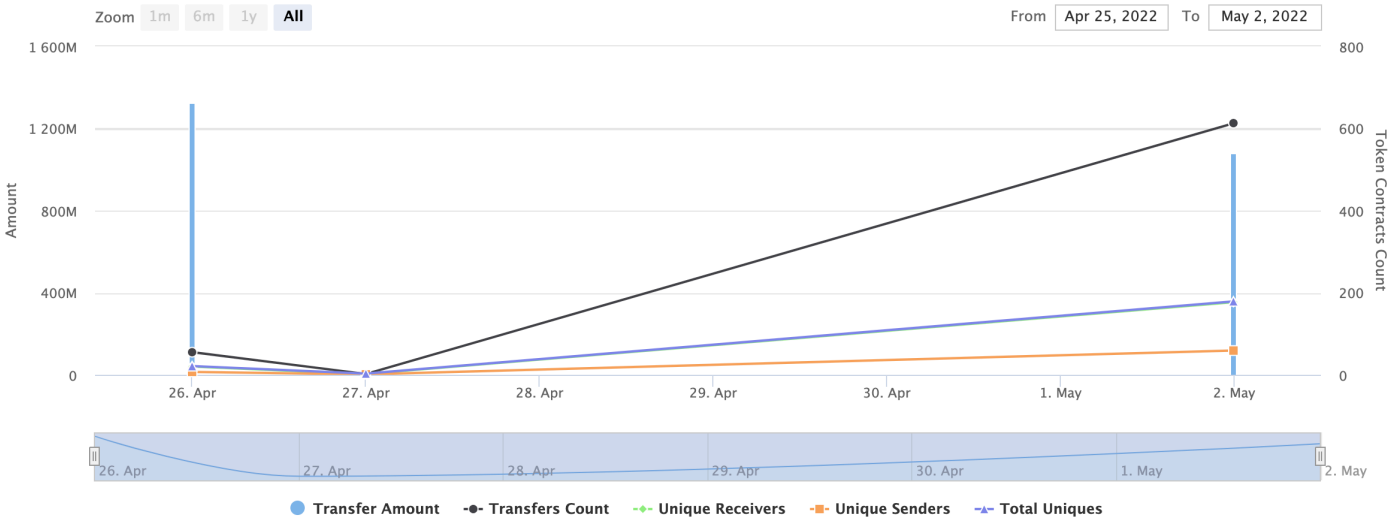
Social Profiles

Project Website: **http://vivy.finance/**

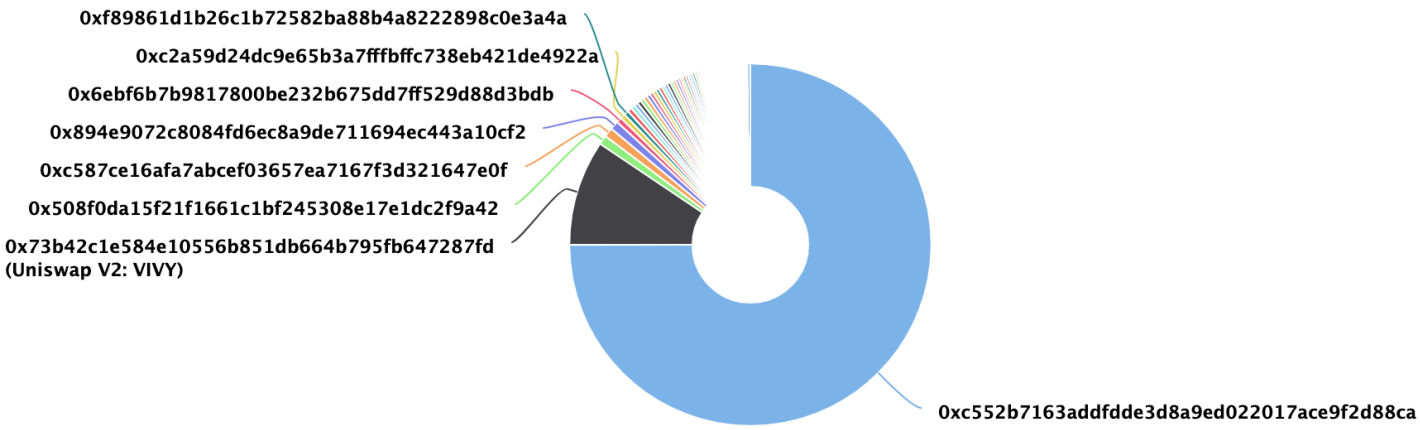
Project Twitter: **https://twitter.com/project_vivy**

Project Telegram: **https://t.me/projectvivy**

Contract Analytics



VIVY Token Distribution



VIVY Top Holders

Rank	Address	Quantity (Token)	Percentage
1	0xc552b7163addfdde3d8a9ed022017ace9f2d88ca	750,000,000	75.0000%
2	Uniswap V2: VIVY	94,122,388.648846193917840453	9.4122%
3	0x508f0da15f21f1661c1bf245308e17e1dc2f9a42	8,303,665.195894096791123856	0.8304%
4	0xc587ce16afa7abcef03657ea7167f3d321647e0f	8,255,662.881517628480692293	0.8256%
5	0x894e9072c8084fd6ec8a9de711694ec443a10cf2	7,758,633.030226820149868093	0.7759%
6	0x6ebf6b7b9817800be232b675dd7ff529d88d3bdb	4,828,084.196171766324190751	0.4828%
7	0xc2a59d24dc9e65b3a7fffbffc738eb421de4922a	4,509,306.314999349686197531	0.4509%
8	0xf89861d1b26c1b72582ba88b4a8222898c0e3a4a	4,095,000.000000000000544834	0.4095%
9	0x73dfada90f1de808da2ba1b4423c331e73e6ac19	4,014,765.938676429680236189	0.4015%
10	0x138a581b2ca20a72b705d88c1cd722d34cb88e2b	3,554,292.266364104556103085	0.3554%

Swap Analysis

✔ Token is sellable (not a honeypot) at this time

✔ Buy fee is <= 10% (9%)

✘ Sell fee is <= 10% (13%)

Contract Analysis

✔ Verified contract source

✘ Ownership renounced or source does not contain an owner contract.

Holder Analysis

✔ Owner/creator wallet contains less than 5% of token supply (0%)

✔ All other holders possess less than 5% of token supply

Contract Analysis

✔ Adequate liquidity present (43.18 ETH)

✔ At least 95% of liquidity burned/locked (100%)

✔ Owner/creator wallet contains less than 5% of liquidity

Project Website Overview

✓ JavaScript errors hasn't been found.
X The SSL certificate is absent
✓ Malware pop-up windows hasn't been detected.
✓ No issues with loading elements, code, or stylesheets.

Project Website Performance Audit

35

Performance

Values are estimated and may vary. The performance score is calculated directly from these metrics. See calculator.

▲ 0–49 ■ 50–89 ● 90–100

RICS Expand v

First Contentful Paint
1.5 s

Time to Interactive
13.4 s

Speed Index
6.5 s

Total Blocking Time
2,980 ms

Largest Contentful Paint
2.1 s

Cumulative Layout Shift
0.026

Project Website Optimization for Mobile

58

Performance

Values are estimated and may vary. The performance score is calculated directly from these metrics. See calculator.

▲ 0–49 ■ 50–89 ● 90–100

ETRICS Expand vie

First Contentful Paint
2.9 s

Time to Interactive
10.0 s

Speed Index
7.5 s

Total Blocking Time
470 ms

Largest Contentful Paint
3.7 s

Cumulative Layout Shift
0.006

Whitepaper of the project

The whitepaper of Vivy project has been verified on behalf of Soken team.

VIVY FINANCE

/ AI-focused investment

Vivy will pursue both on- and off-chain financial solutions for driving project growth and cultivating innovation in the AI and ML space. After careful curation and vetting of projects, the staked Vivy community will have the opportunity to provide feedback and vote on allocation of funds for investment. Returns will be infused back into the project at the benefit of holders.

Verticals that Vivy will pursue include:

- Finance
- Transportation
- Logistics
- Healthcare
- Technology
- Energy
- Entertainment
- Manufacturing
- Advertising
- Commodities

Gartner projects the business value created by AI at $3.9T by 2022.

AI applications do not just have the promise to yield better business results but improve the human experience as a whole.

9 · PROJECT VIVY

Whitepaper link: **http://vivy.finance/vivy_lite_paper.pdf**

Contract Function Details

- [Int] _msgSender
- [Int] _msgData
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer
- [Ext] allowance
- [Ext] approve
- [Ext] transferFrom
- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer
- [Pub] allowance
- [Pub] approve
- [Pub] transferFrom
- [Pub] increaseAllowance
- [Pub] decreaseAllowance
- [Int] _transfer
- [Int] _createInitialSupply
- [Int] _approve
- [Pub] owner
- [Ext] renounceOwnership
- [Pub] transferOwnership
- [Ext] sync
- [Ext] factory
- [Ext] WETH
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens
- [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens
- [Ext] addLiquidityETH
- [Ext] removeLiquidityETH
- [Ext] getAmountsOut
- [Ext] createPair
- [Ext] setGasPriceMax
- [Ext] removeLimits
- [Ext] getEarlyBuyers
- [Ext] removeBoughtEarly
- [Ext] emergencyUpdateRouter

- [Ext] disableTransferDelay
- [Ext] updateMaxBuyAmount
- [Ext] updateMaxSellAmount
- [Ext] updateMaxWallet
- [Ext] updateSwapTokensAtAmount
- [Prv] _excludeFromMaxTransaction
- [Ext] airdropToWallets
- [Ext] excludeFromMaxTransaction
- [Ext] setAutomatedMarketMakerPair
- [Prv] _setAutomatedMarketMakerPair
- [Ext] updateBuyFees
- [Ext] updateSellFees
- [Pub] excludeFromFees
- [Int] _transfer
- [Pub] earlyBuyPenaltyInEffect
- [Prv] swapTokensForEth
- [Ext] getCurrentBlock
- [Ext] getCurrentTimestamp
- [Prv] addLiquidity
- [Prv] swapBack
- [Ext] transferForeignToken
- [Ext] withdrawStuckETH
- [Ext] setOperationsAddress
- [Ext] setTeamAddress
- [Ext] forceSwapBack
- [Ext] launchWithoutAirdrop

Vulnerabilities checking

Issue Description	Checking Status
Compiler Errors	Completed
Delays in Data Delivery	Completed
Re-entrancy	Completed
Transaction-Ordering Dependence	Completed
Timestamp Dependence	Completed
Shadowing State Variables	Completed
DoS with Failed Call	Completed
DoS with Block Gas Limit	Completed
Outdated Complier Version	Completed
Assert Violation	Completed
Use of Deprecated Solidity Functions	Completed
Integer Overflow and Underflow	Completed
Function Default Visibility	Completed
Malicious Event Log	Completed
Math Accuracy	Completed
Design Logic	Completed
Fallback Function Security	Completed
Cross-function Race Conditions	Completed
Safe Zeppelin Module	Completed

Security Issues

1) Owner Privileges

The contract contains ownership functionality and ownership is not renounced which allows the creator or current owner to modify contract behaviour.

2) Controlled Delegate Call : L656

```
653       // withdraw ETH if stuck or someone sends to the address
654       function withdrawStuckETH() external onlyOwner {
655           bool success;
656           (success,) = address(msg.sender).call{value: address(this).balance}("");
657       }
658
```

The contract was using call() which was accepting address controlled by a user. This can have devastating effects on the contract as a delegate call allows the contract to execute code belonging to other contracts but using its own storage. This can very easily lead to a loss of funds and compromise of the contract.

Recommendation:

Do not allow user-controlled data inside the call() function.

Conclusion

Low-severity issues exist within smart contracts. Smart contracts are free from any critical or high-severity issues.

NOTE: Please check the disclaimer above and note, that audit makes no statements or warranties on business model, investment attractiveness or code sustainability.

Soken Contact Info

Website: www.soken.io

Mob: (+1)416-875-4174

32 Britain Street, Toronto, Ontario, Canada

Telegram: @team_soken

GitHub: sokenteam

Twitter: @soken_team