



Smart Contract Security Audit Report

FOCAL POINT

February 2023

Security Status



www.hacksafe.io



Audit Details



Audited project

FOCAL POINT



Deployer address

0x42d290c9338E903efc647FEEe04128e1397B3745



Client contacts

FOCAL POINT Team



Blockchain

Binance smart chain



Website

<https://focaldefi.io/>

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 FOCAL POINT to perform an audit of smart contracts:

- <https://bscscan.com/token/0xF0ca100000e47A0dd2087C81EC910B0BDe6Ad6f5#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 understood to 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.

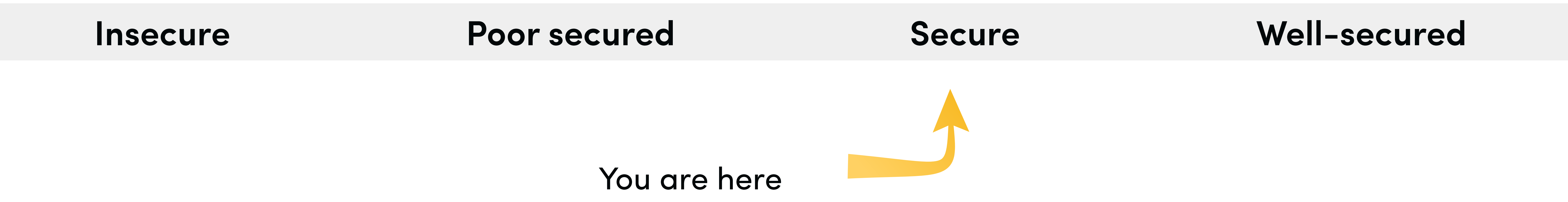
Contract Details

Token contract details for 22.02.2023

Token Type	: DEFI
Contract name	: FocalPoint
Contract address	: 0xF0ca100000e47A0dd2087C81EC910B0BDe6Ad6f5
Total supply	: 15,000,000
Token ticker	: FOCAL
Decimals	: 18
Token Holders	: 117
Transactions count	: 4,944
Compiler version	: v0.8.11+commit.d7f03943
Contract deployer address	: 0x42d290c9338E903efc647FEEe04128e1397B3745
Owner address	: 0x98f6ce7f51e3f2a81982d43859fd43517af2fdac

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.




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.

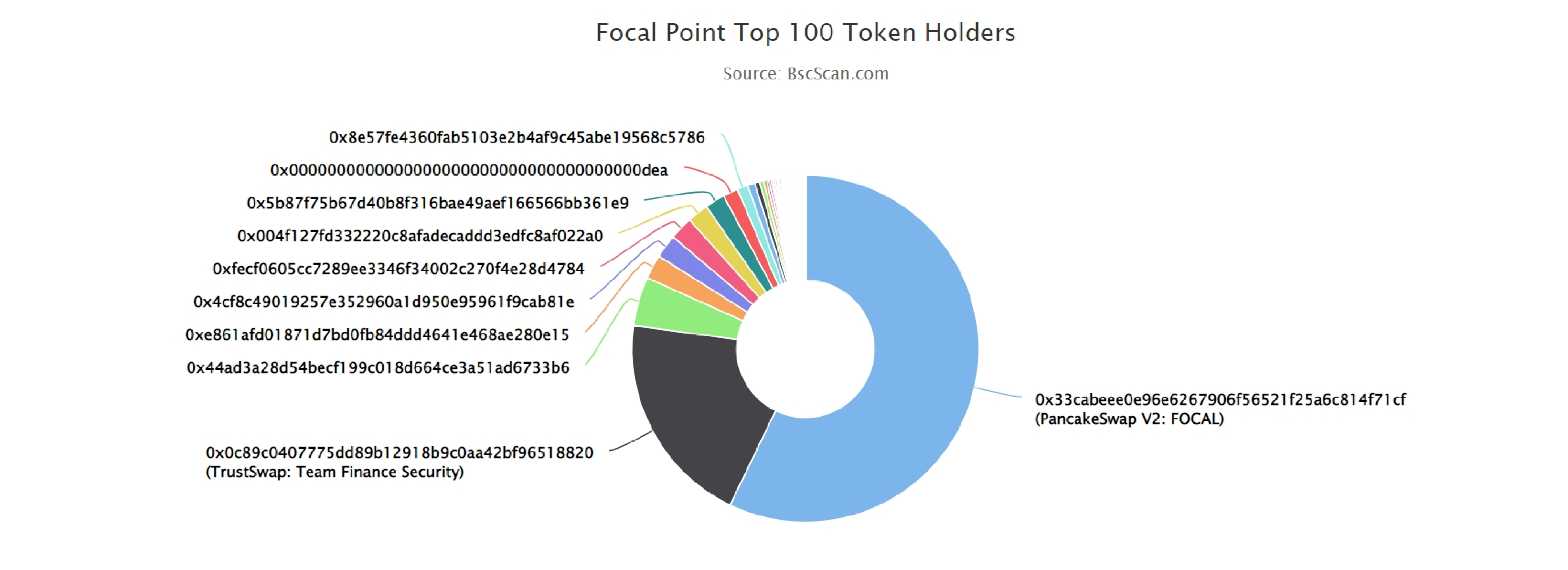
We found 0 critical, 0 high, 0 medium and 0 low.

FOCAL POINT Token Distribution

 The top 100 holders collectively own 100.00% (14,999,977.76 Tokens) of Focal Point






Token Total Supply: 15,000,000.00 Token | Total Token Holders: 117



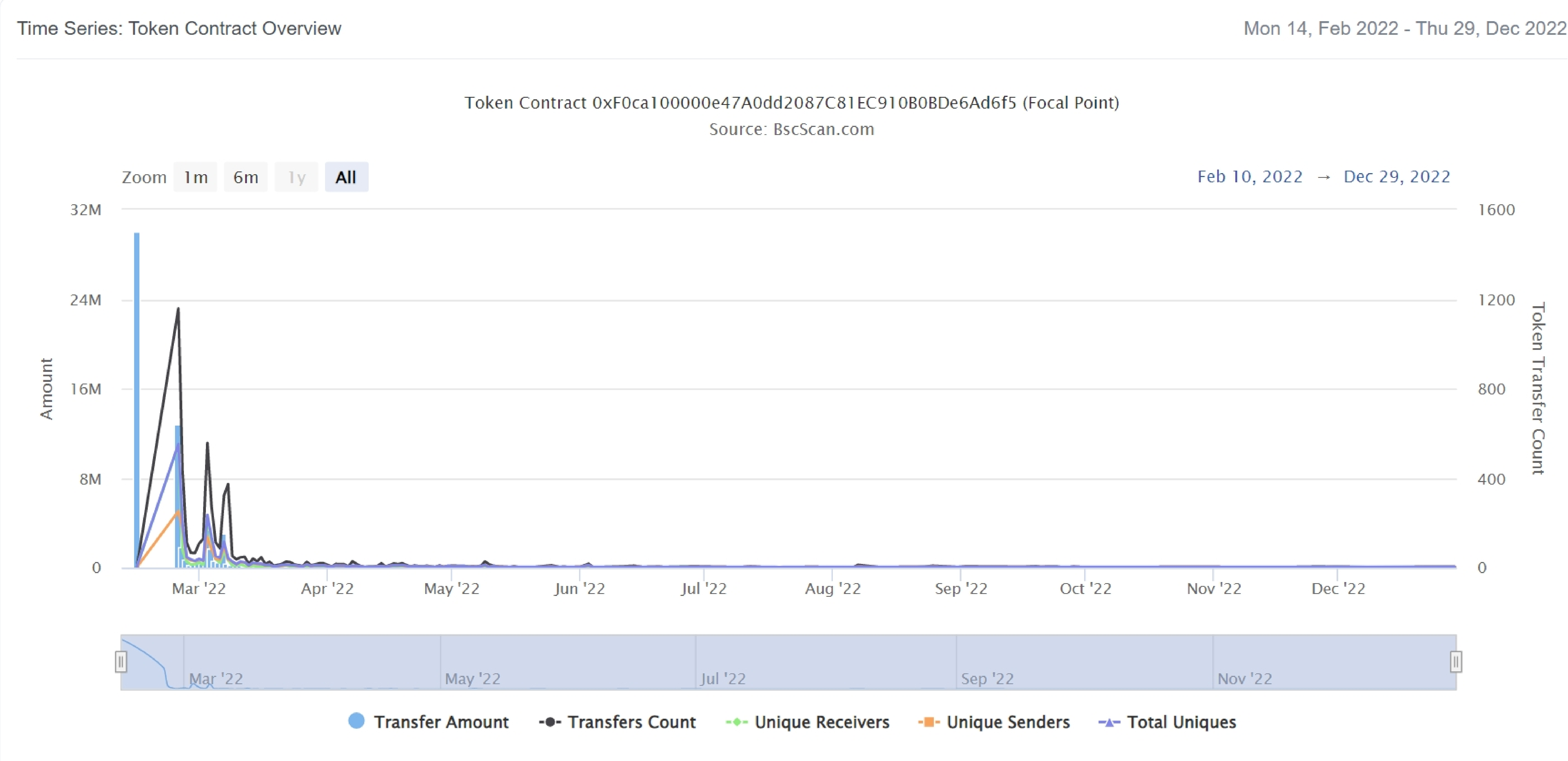
FOCAL POINT Top 01 Token Holders

(A total of 14,999,977.76 tokens held by the top 100 accounts from the total supply of 15,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	 PancakeSwap V2: FOCAL	8,575,408.497926621797898798	57.1694%
2	 TrustSwap: Team Finance Security	3,000,000	20.0000%
3	0x44ad3a28d54becf199c018d664ce3a51ad6733b6	684,175	4.5612%
4	0xe861afd01871d7bd0fb84ddd4641e468ae280e15	336,888.670261110870642419	2.2459%
5	0x4cf8c49019257e352960a1d950e95961f9cab81e	329,419.686156419964813228	2.1961%
6	0xfecf0605cc7289ee3346f34002c270f4e28d4784	328,538.10678421446879889	2.1903%
7	 0x004f127fd332220c8afadecadd3edfc8af022a0	295,958.75	1.9731%
8	0x5b87f75b67d40b8f316bae49aef166566bb361e9	279,987.267399760266011049	1.8666%
9	0x0000000000000000000000000000000000dea	208,364.176404771869866635	1.3891%
10	0x8e57fe4360fab5103e2b4af9c45abe19568c5786	151,255.635610350010854626	1.0084%
11	0x79b88ed0fa351845b0137b0d29b4562eb442af07	103,002.351442491683949666	0.6867%
12	0xdb52703b77c08c83ccb868b3613a2f4814fa1cd9	68,702.307969347146168356	0.4580%
13	0x20eadfa8129c8c4d9cf9a200b9b27ddf818752ac	53,099.06771056954662109	0.3540%
14	0x00f79cb9a6f690ea65407ca1bf123af308bf8328	47,537.944091758416772784	0.3169%
15	0x0281727cc93634a63697ea53852e0fcb341baaa7	33,587.996130409930327658	0.2239%
16	0xd9a98ec628e0d7e5b0957e128134a2fee64ddba7	30,112.141748177936180171	0.2007%
17	0x5cd73c16bee847dc80c9152df7eef323462f1003	25,237.532465861323086372	0.1683%
18	0xe054b622bd70698d0afda69b054bbc996e9e1154	23,160.246732842662603704	0.1544%
19	0x242762d421ed5ee7a2626a040d44a26a7bcb075d	22,450	0.1497%
20	0xa7f532a90897a980d6a1db0adc6522fa683b1a37	22,450	0.1497%

FOCAL POINT Token Distribution

FOCAL POINT Contract overview



Contract functions details

+[Int] IERC20Metadata (IERC20)

- [Ext] name
- [Ext] symbol
- [Ext] decimals

+[Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+Context

- [Int] _msgSender
- [Int] _msgData

+[Int] ISwapFactory

- [Ext] createPair #

+[Int] ISwapRouter

- [Ext] addLiquidityETH (\$)
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
- [Ext] factory
- [Ext] WETH

+ERC20 (Context, IERC20, IERC20Metadata)

- [Pub] <Constructor> #
- [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] _mint #

Contract functions details

- [Int] _burn #
- [Int] _approve #
- [Int] _beforeTokenTransfer #
- [Int] _afterTokenTransfer #

+Ownable (Context)

- [Pub] <Constructor>#
- [Pub] owner
- [Pub] renounceOwnership #
 - modifiers: onlyOwner
- [Pub] transferOwnership #
 - modifiers: onlyOwner
- [Int] _transferOwnership #

+FocalPoint (ERC20, Ownable)

- [Pub] <Constructor>#
 - modifiers: ERC20
- [Ext] <Fallback >(\$)
- [Pub] enableTrading #
 - modifiers: onlyOwner
- [Pub] enableFees #
 - modifiers: onlyOwner
- [Pub] setFeeless #
 - modifiers: onlyOwner
- [Ext] buyFee
- [Ext] sellFee
- [Pub] setFeeAddresses #
 - modifiers: onlyOwner
- [Pub] setBuyFees #
 - modifiers: onlyOwner
- [Pub] setSellFees #
 - modifiers: onlyOwner
- [Pub] setMinSwapTokens #
 - modifiers: onlyOwner
- [Pub] setMaxTransaction #
 - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
 - modifiers: onlyOwner
- [Int] _transfer #

Contract functions details

- [Pvt] _calculateTokensForFee
- [Pvt] _getTransferType
- [Pvt] _buyTransfer #
- [Pvt] _feesForDistributeCollected
- [Pvt] _sellTransfer #
- [Pvt] _swapAndDistribute #
 - modifiers: lockTheSwap
- [Pvt] _swapAndLiquify #
 - modifiers: lockTheSwap
- [Pvt] _swapTokensForNative #
- [Pvt] _addLiquidity #

(\$) = 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.	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

No low severity issue found.

Centralization

Owner privileges :

- FOCAL POINT Contract:
 - Owner can enable trading.
 - Owner can enable/disable fees.
 - Owner can make addresses feeless.
 - Owner can change fees.
 - Owner can change the maximum transaction and minimum swap amounts.

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.

Conclusion

Smart contract contains no 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.