Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

August, 2021

Audit Details

Audited project

SPHYNX

Deployer address

0x6f8A6F92087EEAd810672C1A27647530Ea7Fc81C

Client contacts:

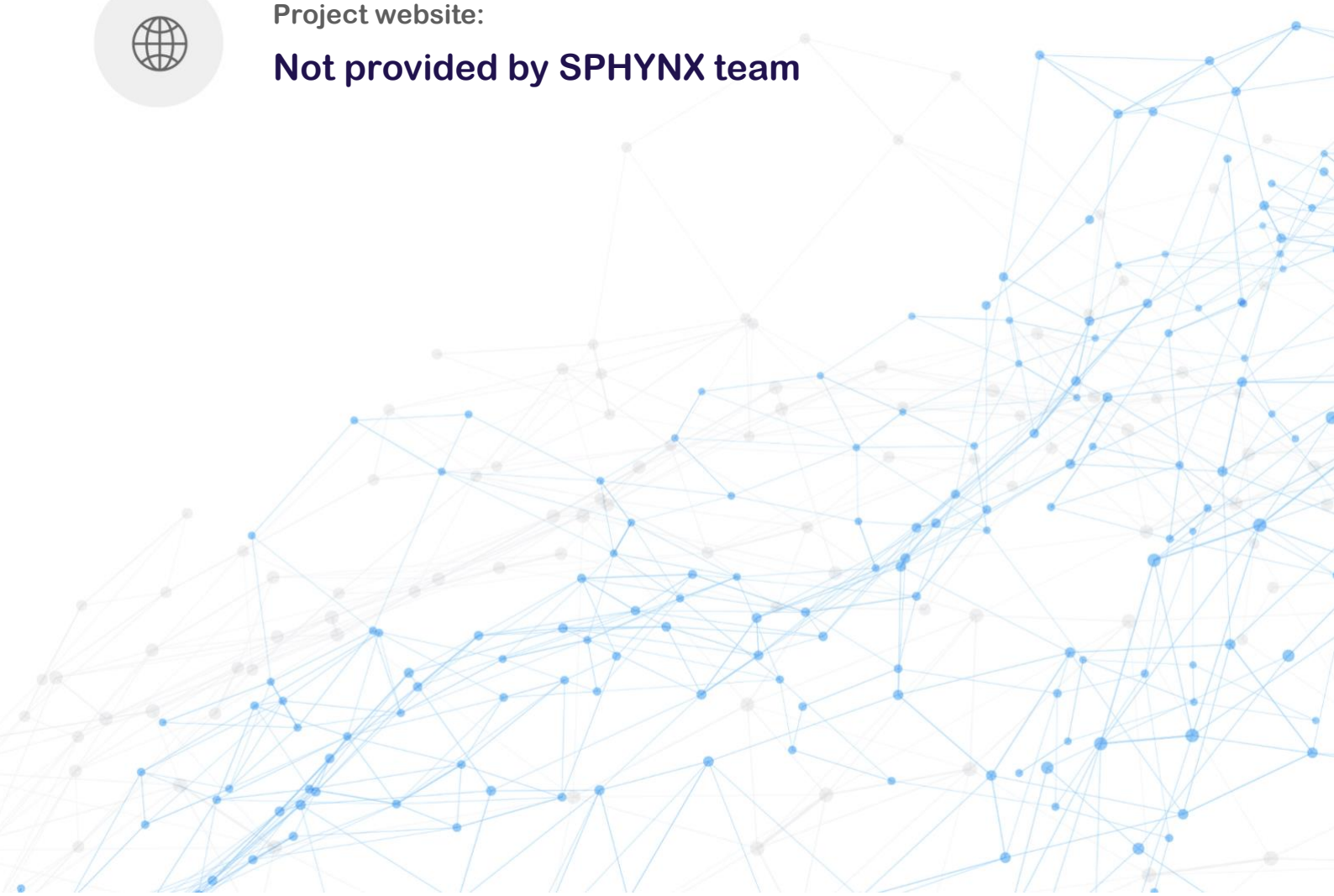
SPHYNX team

Blockchain

Binance Smart Chain

Project website:

Not provided by SPHYNX 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) (TechRate) owe no duty of care towards you or any other person, nor does TechRate 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 TechRate 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, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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

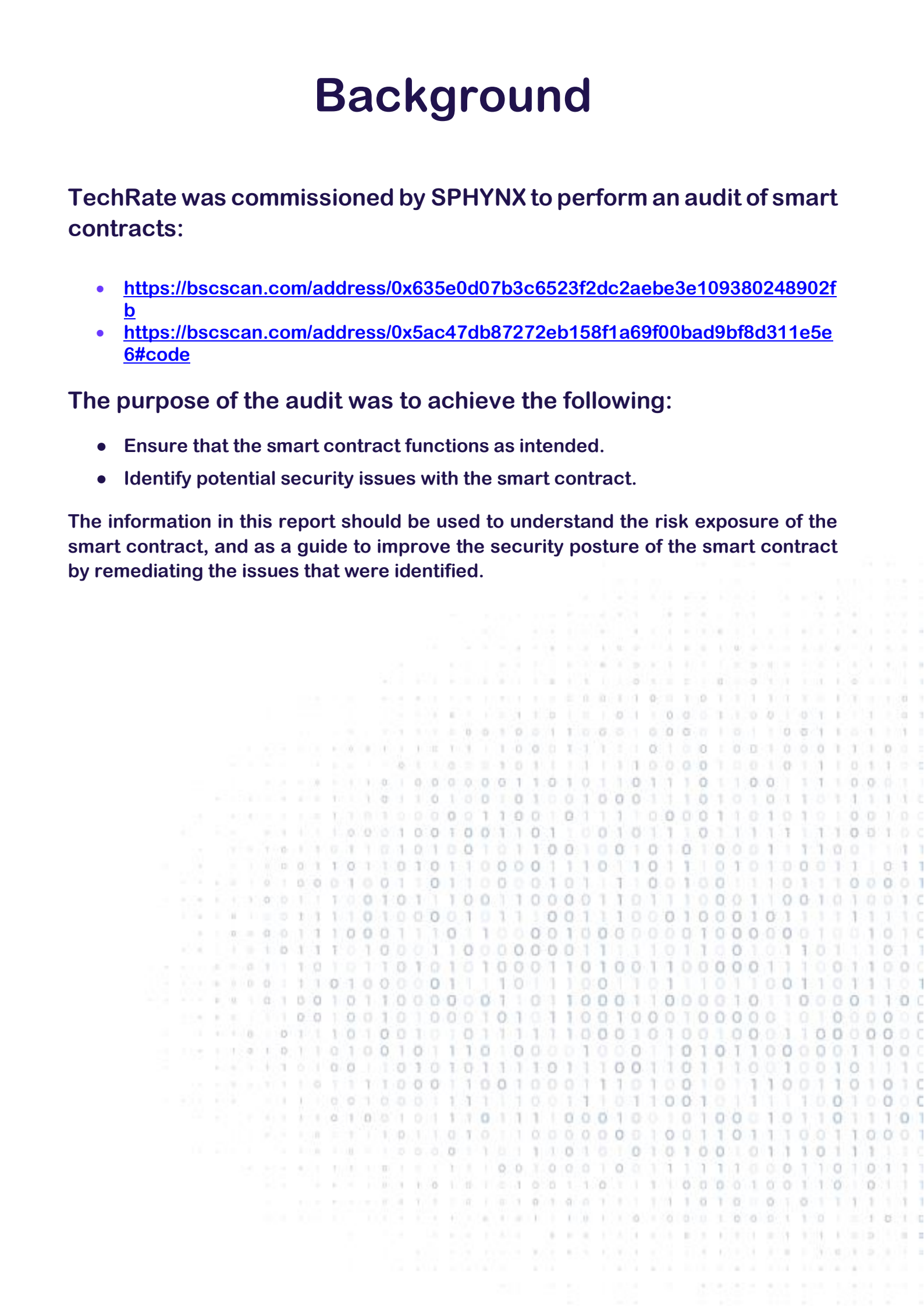
TechRate was commissioned by SPHYNX to perform an audit of smart contracts:

- https://bscscan.com/address/0x635e0d07b3c6523f2dc2aebe3e109380248902fb
- https://bscscan.com/address/0x5ac47db87272eb158f1a69f00bad9bf8d311e5e6#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 used 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.



Contracts Details

Token contract details for 15.08.2021

Contract name	SphynxRouter01/ SphynxFactory
Contract addresses	0x5AC47dB87272EB158f1A69f00BAD9Bf8D311E5E6 0x635e0D07b3C6523f2Dc2aEbE3E109380248902fb
Factory	0x635e0D07b3C6523f2Dc2aEbE3E109380248902fb
Router	0x5AC47dB87272EB158f1A69f00BAD9Bf8D311E5E6
WETH	0xbb4cdb9cbd36b01bd1cbaebf2de08d9173bc095c
Fee too	0x0000000000000000000000000000000000000000
Fee to setter	0x795bab595218150833bc4bbc96541d37ed7658cf
All pairs length	1
Contract deployer address	0x6f8A6F92087EEAd810672C1A27647530Ea7Fc81C

Contract SphynxFactory functions details

+ [Int] ISphynxFactory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #
  - [Ext] setSwapFee #

+ [Int] ISphynxPair
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transfer #
  - [Ext] transferFrom #
  - [Ext] DOMAIN_SEPARATOR
  - [Ext] PERMIT_TYPEHASH
  - [Ext] nonces
  - [Ext] permit #
  - [Ext] MINIMUM_LIQUIDITY
  - [Ext] factory
  - [Ext] token0
  - [Ext] token1
  - [Ext] getReserves
  - [Ext] price0CumulativeLast
  - [Ext] price1CumulativeLast
  - [Ext] kLast
  - [Ext] swapFee
  - [Ext] mint #
  - [Ext] burn #
  - [Ext] swap #
  - [Ext] skim #
  - [Ext] sync #
  - [Ext] initialize #
  - [Ext] setSwapFee #

+ [Int] ISphynxERC20
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] allowance

  - [Ext] approve #
  - [Ext] transfer #
  - [Ext] transferFrom #
  - [Ext] DOMAIN_SEPARATOR
  - [Ext] PERMIT_TYPEHASH
  - [Ext] nonces
  - [Ext] permit #

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

+ SphynxERC20 (ISphynxERC20)
  - [Pub] <Constructor> #
  - [Int] _mint #
  - [Int] _burn #
  - [Prv] _approve #
  - [Prv] _transfer #
  - [Ext] approve #
  - [Ext] transfer #
  - [Ext] transferFrom #
  - [Ext] permit #

+ [Lib] Math
  - [Int] min
  - [Int] sqrt

+ [Lib] UQ112x112
  - [Int] encode
  - [Int] uqdiv

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

+ [Int] ISphynxCallee
  - [Ext] sphynxCall #

+ SphynxPair (ISphynxPair, SphynxERC20)
  - [Pub] getReserves
  - [Prv] _safeTransfer #
  - [Pub] <Constructor> #
  - [Ext] initialize #
  - [Ext] setSwapFee #
  - [Prv] _update #
  - [Prv] _mintFee #
  - [Ext] mint #

    - modifiers: lock
  - [Ext] burn #
    - modifiers: lock
  - [Ext] swap #
    - modifiers: lock
  - [Ext] skim #
    - modifiers: lock
  - [Ext] sync #
    - modifiers: lock

+ SphynxFactory (ISphynxFactory)
  - [Pub] <Constructor> #
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #
  - [Ext] setSwapFee #

($) = payable function
= non-constant function

Contract SphynxRouter01 functions details

+ [Int] ISphynxFactory
  - [Ext] feeTo
  - [Ext] swapFee
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setSwapFee #
  - [Ext] setFeeToSetter #

+ [Lib] TransferHelper
  - [Int] safeApprove #
  - [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeTransferETH #

+ [Int] ISphynxPair
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transfer #
  - [Ext] transferFrom #
  - [Ext] DOMAIN_SEPARATOR
  - [Ext] PERMIT_TYPEHASH
  - [Ext] nonces
  - [Ext] permit #
  - [Ext] MINIMUM_LIQUIDITY
  - [Ext] factory
  - [Ext] token0
  - [Ext] token1
  - [Ext] getReserves
  - [Ext] price0CumulativeLast
  - [Ext] price1CumulativeLast
  - [Ext] kLast
  - [Ext] swapFee
  - [Ext] mint #
  - [Ext] burn #
  - [Ext] swap #
  - [Ext] skim #
  - [Ext] sync #
  - [Ext] initialize #

+ [Lib] SafeMath

  - [Int] add
  - [Int] sub
  - [Int] mul

+ [Lib] SphynxLibrary
  - [Int] sortTokens
  - [Int] pairFor
  - [Int] getSwapFee
  - [Int] getReserves
  - [Int] quote
  - [Int] getAmountOut
  - [Int] getAmountIn
  - [Int] getAmountsOut
  - [Int] getAmountsIn

+ [Int] ISphynxRouter01
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] removeLiquidity #
  - [Ext] removeLiquidityETH #
  - [Ext] removeLiquidityWithPermit #
  - [Ext] removeLiquidityETHWithPermit #
  - [Ext] swapExactTokensForTokens #
  - [Ext] swapTokensForExactTokens #
  - [Ext] swapExactETHForTokens ($)
  - [Ext] swapTokensForExactETH #
  - [Ext] swapExactTokensForETH #
  - [Ext] swapETHForExactTokens ($)
  - [Ext] quote
  - [Ext] getAmountOut
  - [Ext] getAmountIn
  - [Ext] getAmountsOut
  - [Ext] getAmountsIn

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

+ [Int] IWETH
  - [Ext] deposit ($)
  - [Ext] transfer #
  - [Ext] withdraw #

+ SphynxRouter01 (ISphynxRouter01)
  - [Pub] <Constructor> #
  - [Ext] <Fallback> ($)

- [Prv] _addLiquidity #
- [Ext] addLiquidity #
  - modifiers: ensure
- [Ext] addLiquidityETH ($)
  - modifiers: ensure
- [Pub] removeLiquidity #
  - modifiers: ensure
- [Pub] removeLiquidityETH #
  - modifiers: ensure
- [Ext] removeLiquidityWithPermit #
- [Ext] removeLiquidityETHWithPermit #
- [Prv] _swap #
- [Ext] swapExactTokensForTokens #
  - modifiers: ensure
- [Ext] swapTokensForExactTokens #
  - modifiers: ensure
- [Ext] swapExactETHForTokens ($)
  - modifiers: ensure
- [Ext] swapTokensForExactETH #
  - modifiers: ensure
- [Ext] swapExactTokensForETH #
  - modifiers: ensure
- [Ext] swapETHForExactTokens ($)
  - modifiers: ensure
- [Pub] quote
- [Pub] getAmountOut
- [Pub] getAmountIn
- [Pub] getAmountsOut
- [Pub] getAmountsIn

($) = payable function
= non-constant function

Issues Checking Status

	Issue description	Checking status
1.	Compiler errors.	Passed
2.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3.	Possible delays in data delivery.	Passed
4.	Oracle calls.	Passed
5.	Front running.	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.	The impact of the exchange rate on the logic.	Passed
13.	Private user data leaks.	Passed
14.	Malicious Event log.	Passed
15.	Scoping and Declarations.	Passed
16.	Uninitialized storage pointers.	Passed
17.	Arithmetic accuracy.	Passed
18.	Design Logic.	Passed
19.	Cross-function race conditions.	Passed
20.	Safe Open Zeppelin contracts implementation and usage.	Passed
21.	Fallback function security.	Passed

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

No low severity issues found.

Conclusion

Smart contracts do not contain high severity issues!

TechRate 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.