

Auditoria de Segurança de Contrato Inteligente

Detalhes da auditoria:

Projeto auditadot: BODA

Endereço do Implantador: 0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede

Contatos do cliente: BODA team

Blockchain: Binance Smart Chain

Site do projeto: https://www.bodatoken.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) (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.

Histórico

A TechRate foi contratada pelo BODA para realizar uma auditoria de contratos inteligentes:

• <u>https://bscscan.com/address/0x81cfb5e400eb2caa319130a0dae3b32cfb1939</u> 2d#code

O objetivo da auditoria era alcançar o seguinte:

- Certificar-se que o contrato inteligente funciona conforme pretendido.
- Identificar possíveis problemas de segurança com o contrato inteligente.

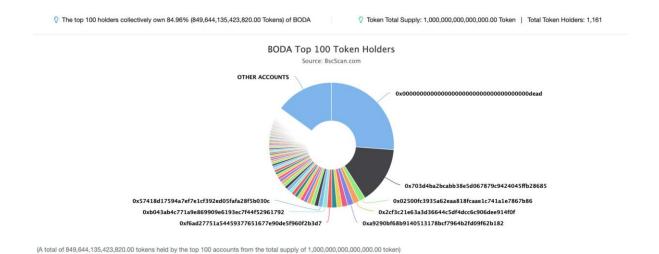
As informações neste relatório devem ser usadas para entender a exposição ao risco do contrato inteligente e como um guia para melhorar a postura de segurança do contrato inteligente corrigindo os problemas que foram identificados.

Detalhes de contratos

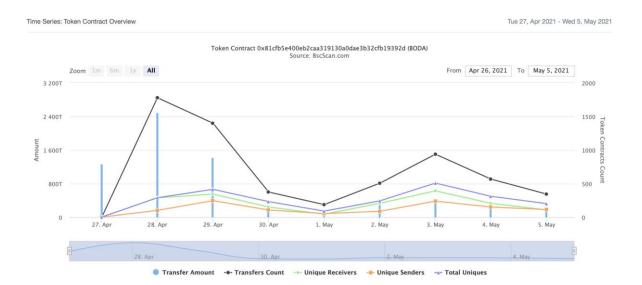
Detalhes do contrato de token para 06.05.2021.

Nome do contrato:	BODA
Endereço do contrato:	0x81cfb5e400eb2caa319130a0dae3b32cfb19392d
Oferta total:	1_000_000_000_000_000_000
Token ticker:	BODA
Decimais:	9
Detentores de token:	1161
Contagem de transações:	6645
Domínio dos 100 principais detentores::	84.96 %
Taxa de liquidez:	7
Taxa de imposto::	3
Total de taxas:	158_388_874_733_266_276_146_654
Par PancakeSwap V2:	0x703d4ba2bcabb38e5d067879c9424045ffb28685
Endereço do implantador do contrato:	0x4acd5d62f01f13a397e5bf5cdf8f4c0a69534ede
Endereço atual do proprietário do contrato:	0x000000000000000000000000000000000000

Distribuição de tokens BODA



Detalhes de interação do contrato BODA



10 principais detentores de tokens

Rank	Address	Quantity (Token)	Percentage
1	0x000000000000000000000000000000000000	261,846,632,068,150.734795191	26.1847%
2	₫ 0x703d4ba2bcabb38e5d067879c9424045ffb28685	148,093,423,272,344.214316344	14.8093%
3	0x02500fc3935a62eaa818fcaae1c741a1e7867b86	16,182,538,750,959.627114805	1.6183%
4	0x2cf3c21e63a3d36644c5df4dcc6c906dee914f0f	16,003,463,057,035.183010255	1.6003%
5	0xa9290bf68b9140513178bcf7964b2fd09f62b182	15,949,136,925,840.478166507	1.5949%
6	0x8d76fe4578852c3bebd2034564daf3ded4d98406	14,493,183,093,023.014186082	1.4493%
7	0xe0d65e3741f1beea47cdf6a5a60cf9ef9fb8411b	13,508,986,903,972.547580741	1.3509%
8	0xf4e0e6dee785e8836f09986e1e15b6d9acc14e3d	13,019,975,334,181.42316904	1.3020%
9	0xf6ad27751a54459377651677e90de5f960f2b3d7	12,313,988,838,945.639751371	1.2314%
10	0xb043ab4c771a9e869909e6193ec7f44f52961792	11,689,496,228,270.477698551	1.1689%

Detentores de tokens BODA LP

Rank	Address	Quantity	Percentage
1	ⓑ 0x00000000000000000000000000000000000	2,778.151297143223770026	83.9943%
2	0x000000000000000000000000000000000000	503.785866355147604036	15.2314%
3	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	24.902359302611641429	0.7529%
4	0xe9eff515b9e29c393af69d3c5905458de54fde5a	0.70863107114452575	0.0214%

Detalhes das funções do contrato

+ [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
- [Int] mod
- [Int] mod

+ Context

- [Int] _msgSender
- [Int] _msgData

+ [Lib] Address

- [Int] isContract
- [Int] sendValue #
- [Int] functionCall #
- [Int] functionCall #
- [Int] functionCallWithValue #
- [Int] functionCallWithValue #
- [Prv] _functionCallWithValue #

+ Ownable (Context)

- [Int] <Constructor> #
- [Pub] owner
- [Pub] renounceOwnership #
 - modifiers: onlyOwner
- [Pub] transferOwnership #
 - modifiers: onlyOwner
- [Pub] geUnlockTime
- [Pub] lock #
 - modifiers: onlyOwner
- [Pub] unlock #

- [Ext] feeTo
- [Ext] feeToSetter
- [Ext] getPair
- [Ext] all Pairs
- [Ext] allPairsLength
- [Ext] createPair #
- [Ext] setFeeTo #
- [Ext] setFeeToSetter #

+ [Int] IUniswapV2Pair

- [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] mint #
- [Ext] burn#
- [Ext] swap #
- [Ext] skim #
- [Ext] sync #
- [Ext] initialize #

+ [Int] IUniswapV2Router01

- [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] IUniswapV2Router02 (IUniswapV2Router01)
 - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
 - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
 - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
 - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens (\$)
 - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
- + BODA (Context, IERC20, Ownable)
 - [Pub] <Constructor>#
 - [Pub] name
 - [Pub] symbol
 - [Pub] decimals
 - [Pub] totalSupply
 - [Pub] balanceOf
 - [Pub] transfer #
 - [Pub] allowance
 - [Pub] approve #
 - [Pub] transferFrom #
 - [Pub] increaseAllowance #
 - [Pub] decreaseAllowance #
 - [Pub] isExcludedFromReward
 - [Pub] totalFees
 - [Pub] deliver #
 - [Pub] reflectionFromToken
 - [Pub] tokenFromReflection
 - [Pub] excludeFromReward #
 - modifiers: onlyOwner
- [Ext] includeInReward #
 - modifiers: onlyOwner
 - [Prv] _transferBothExcluded #
 - [Pub] excludeFromFee #
 - modifiers: onlyOwner
 - [Pub] includeInFee #
- modifiers: onlyOwner
- [Ext] setTaxFeePercent #

- modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
 - modifiers: onlyOwner
- [Ext] setMaxTxPercent#
 - modifiers: onlyOwner
 - [Pub] setSwapAndLiquifyEnabled #
 - modifiers: onlyOwner
 - [Ext] <Fallback> (\$)
 - [Prv] _reflectFee #
 - [Prv] _getValues
 - [Prv] getTValues
 - [Prv]_getRValues
 - [Prv] _getRate
 - [Prv] _getCurrentSupply
 - [Prv] _takeLiquidity #
 - [Prv] calculateTaxFee
 - [Prv] calculateLiquidityFee
 - [Prv] removeAllFee #
 - [Prv] restoreAllFee#
 - [Pub] isExcludedFromFee
 - [Prv] _approve #
 - [Prv]_transfer#
 - [Prv] swapAndLiquify #
 - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
 - [Prv] addLiquidity #
 - [Prv] _tokenTransfer #
 - [Prv] _transferStandard #
 - [Prv] _transferToExcluded #
 - [Prv] _transferFromExcluded #

(\$) = payable function

= non-constant function

Problemas de Verificação de Status

Nº	Descrição do problema.	Status da verificação
1	Erros de compilação.	Aprovado
2	Condições de corrida e Reentrada. Condições de corrida de função cruzada.	Aprovado
3	Possíveis atrasos na entrega de dados.	Aprovado
4	Oracle calls.	Aprovado
5	Corrida frontal.	Aprovado
6	Dependência do timestamp.	Aprovado
7	Excesso e Deficiência de Inteiros.	Aprovado
8	DoS com Reversão.	Aprovado
9	DoS com limite de gás de blocos.	Problemas pequenos
10	Permissões de execução de métodos.	Aprovado
11	Modelo de economia do contrato.	Aprovado
12	O impacto da taxa de câmbio na lógica.	Aprovado
13	Vazamentos de dados privados do usuário.	Aprovado
14	Registro de eventos maliciosos.	Aprovado
15	Escopo e Declarações.	Aprovado
16	Ponteiros de armazenamento não inicializados.	Aprovado
17	Precisão aritmética.	Aprovado
18	Lógica de design.	Aprovado
19	Condições de corrida de função cruzada.	Aprovado
20	Implementação e uso de contratos Safe Open Zeppelin.	Aprovado
21	Segurança da função reserva.	Aprovado

Problemas de Segurança

Problemas de Alta Gravidade

Nenhum problema de alta gravidade encontrado.

Problemas de Gravidade Média

Nenhum problema de gravidade média encontrado.

Problemas de Baixa Gravidade

1. Sem gás

Problema:

☐ A função includeInReward() usa o loop para localizar e remover endereços da lista _ excluded. A função será abortada com exceção OUT_OF_GAS se houver uma longa lista de endereços excluídos.

 □ A função _ getCurrentSupply também usa o loop para avaliar o fornecimento total. Também pode ser abortado com exceção
OUT_OF_GAS se houver uma longa lista de endereços excluídos

Recomendação: Use EnumerableSet em vez de array ou não use arrays longos.

Conclusion

Smart contracts do not contain high severity issues! Liquidity pair contract's security is not checked due to out of scope.

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.