February, 2022

TechRate

AUDIT COMPANY

Smart Contract Security Audit

Audit Details

Audited project
Everath

Deployer address
0xe823646c4f0e0f4fcd4198aa5145cd40921c57ee

Client contacts:
Everath team

Blockchain
Binance Smart Chain

Project website:
https://everath.com/

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 Everath to perform an audit of smart contracts:

https://bscscan.com/address/0x5827A07BA092C1ef586765B9A133F3e7E3da985E#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 23.02.2022

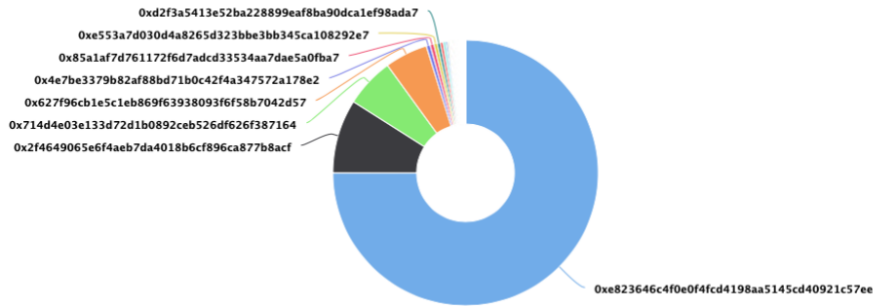|	
Contract name	Everath
Contract address	0x5827A07BA092C1ef586765B9A133F3e7E3da985E
Total supply	100,000,000
Token ticker	EATH
Decimals	18
Token holders	86
Transactions count	134
Top 100 holders dominance	100.00%
Liquidity fee	1
Tax fee	1
Penalty fee	35
Uniswap V2 pair	0x00284c3e5b974ab2aaaffa8fdd018fe430aac47d
Contract deployer address	0xe823646c4f0e0f4fcd4198aa5145cd40921c57ee
Contract's current owner address	0xe823646c4f0e0f4fcd4198aa5145cd40921c57ee

Everath Token Distribution

Everath Top 100 Token Holders
Source: BscScan.com

0xd2f3a5413e52ba228899eaf8ba90dca1ef98ada7
0xe553a7d030d4a8265d323bbe3bb345ca108292e7
0x85a1af7d761172f6d7adcd33534aa7dae5a0fba7
0x4e7be3379b82af88bd71b0c42f4a347572a178e2
0x627f96cb1e5c1eb869f63938093f6f58b7042d57
0x714d4e03e133d72d1b0892ceb526df626f387164
0x2f4649065e6f4aeb7da4018b6cf896ca877b8acf

0xe823646c4f0e0f4fcd4198aa5145cd40921c57ee

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

Everath Contract Interaction Details

Token Contract 0x5827A07BA092C1ef586765B9A133F3e7E3da985E (Everath)
Source: BscScan.com

Zoom 1m 6m 1y All   From Feb 13, 2022 To Feb 21, 2022

● Transfer Amount   -●- Transfers Count   -●- Unique Receivers   -■- Unique Senders   -▲- Total Uniques
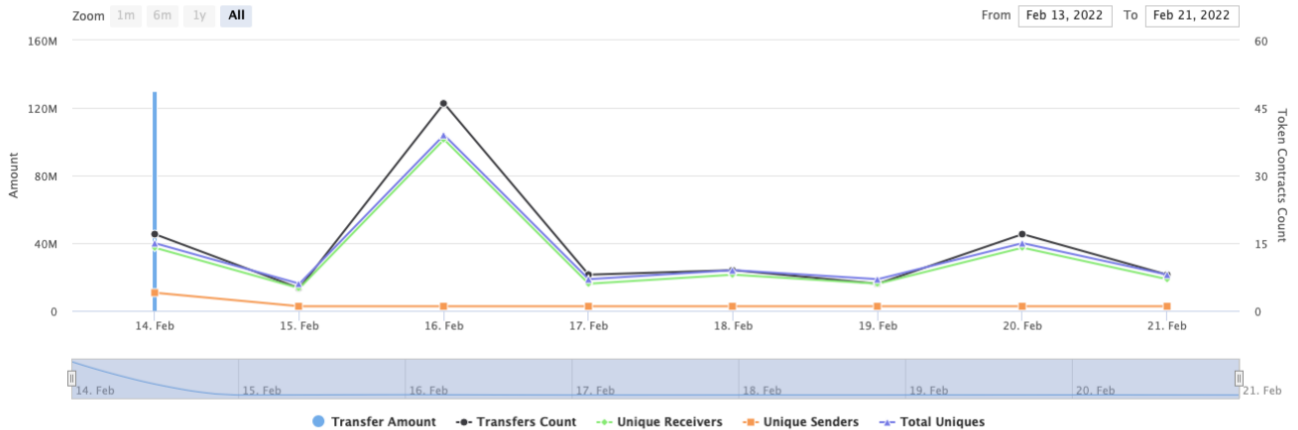
Everath Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xe823646c4f0e0f4fcd4198aa5145cd40921c57ee	75,000,000	75.0000%
2	0x2f4649065e6f4aeb7da4018b6cf896ca877b8acf	9,000,000	9.0000%
3	0x714d4e03e133d72d1b0892ceb526df626f387164	6,000,000	6.0000%
4	📄 0x627f96cb1e5c1eb869f63938093f6f58b7042d57	5,212,671.850826699080023376	5.2127%
5	0x4e7be3379b82af88bd71b0c42f4a347572a178e2	485,773.689542807742232999	0.4858%
6	0x85a1af7d761172f6d7adcd33534aa7dae5a0fba7	456,268.696265702431937332	0.4563%
7	0xe553a7d030d4a8265d323bbe3bb345ca108292e7	413,340.766496356406718997	0.4133%
8	0xd2f3a5413e52ba228899eaf8ba90dca1ef98ada7	365,282.555867023409564666	0.3653%
9	0xa6d124dede4a128305950bead371f7b841e5e3c1	332,988.791604600733359666	0.3330%
10	0xab80a6eb649020e1ec8233e2efc20c280ea154f4	324,737.485835717937892333	0.3247%

Contract functions details

+ Context
  - **[Int]** _msgSender
  - **[Int]** _msgData

+ [Int] IUniswapV2Factory
  - **[Ext]** feeTo
  - **[Ext]** feeToSetter
  - **[Ext]** getPair
  - **[Ext]** allPairs
  - **[Ext]** allPairsLength
  - **[Ext]** createPair **#**
  - **[Ext]** setFeeTo **#**
  - **[Ext]** setFeeToSetter **#**

+ [Int] IBEP20
  - **[Ext]** totalSupply
  - **[Ext]** balanceOf
  - **[Ext]** transfer **#**
  - **[Ext]** allowance
  - **[Ext]** approve **#**
  - **[Ext]** transferFrom **#**

+ [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 **#**

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue **#**
  - [Int] functionCall **#**
  - [Int] functionCall **#**
  - [Int] functionCallWithValue **#**
  - [Int] functionCallWithValue **#**
  - **[Prv]** _functionCallWithValue **#**

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

+ Ownable (Context)
  - [Int] <Constructor> **#**
  - **[Pub]** owner
  - **[Pub]** presaleContract
  - **[Pub]** oracleManager
  - **[Pub]** renounceOwnership **#**
    - modifiers: onlyOwner
  - **[Pub]** transferOwnership **#**

- modifiers: onlyOwner
    - [Int] _transferOwnership #
    - [Pub] transferOracleManager #
      - modifiers: onlyOwner
    - [Int] _transferOracleManager #
    - [Pub] transferPresaleContract #
      - modifiers: onlyOwner
    - [Int] _transferPresaleContract #
    - [Pub] geUnlockTime
    - [Pub] lockOwnerForTime #
      - modifiers: onlyOwner
    - [Pub] unlockOwner #

  + everath (Context, IBEP20, Ownable)
    - [Pub] <Constructor> #
    - [Pub] setSpecialPresaleState #
      - modifiers: onlyOwner
    - [Pub] setBuyerSpecialPresale #
      - modifiers: onlyPresaleContract
    - [Pub] setBuyerSpecialPresaleByOwner #
      - modifiers: onlyOwner
    - [Pub] getBuyerSpecialPresale
    - [Pub] name
    - [Pub] symbol
    - [Pub] decimals
    - [Pub] totalSupply
    - [Pub] balanceOf
    - [Pub] transfer #
    - [Pub] allowance
    - [Pub] approve #
    - [Pub] transferFrom #
    - [Pub] increaseAllowance #
    - [Pub] decreaseAllowance #
    - [Pub] deliver #
    - [Pub] totalFees
    - [Pub] setswapState #
      - modifiers: onlyOwner
    - [Ext] setSwapTokensAtAmount #
      - modifiers: onlyOwner
    - [Ext] setMaxTxPercent #
      - modifiers: onlyOwner
    - [Pub] excludeFromReward #
      - modifiers: onlyOwner
    - [Ext] includeInReward #
      - modifiers: onlyOwner
    - [Pub] isExcludedFromReward
    - [Pub] excludeFromFee #
      - modifiers: onlyOwner
    - [Pub] includeInFee #
      - modifiers: onlyOwner
    - [Pub] isExcludedFromFee
    - [Ext] setOracleGasFeeAddress #
      - modifiers: onlyOwner
    - [Ext] set_feesEnabled #
      - modifiers: onlyOwner

- **[Ext]** setLiquidityFeePercent **#**
  - modifiers: onlyOwner
- **[Ext]** setTaxFeePercent **#**
  - modifiers: onlyOwner
- **[Ext]** setPenaltyFeePercent **#**
  - modifiers: onlyOwner
- **[Pub]** updateUniswapV2Router **#**
  - modifiers: onlyOwner
- **[Pub]** setAutomatedMarketMakerPair **#**
  - modifiers: onlyOwner
- **[Prv]** _setAutomatedMarketMakerPair **#**
- **[Pub]** blackList **#**
  - modifiers: onlyOwner
- **[Pub]** removeFromBlacklist **#**
  - modifiers: onlyOwner
- **[Pub]** checkBlackList
  - modifiers: onlyOwner
- **[Ext]** lockContract_state **#**
  - modifiers: onlyOwner
- **[Ext]** Sweep **#**
  - modifiers: onlyOwner
- **[Pub]** transferForeignToken **#**
  - modifiers: onlyOwner
- **[Ext]** set_stopSellsState_owner **#**
  - modifiers: onlyOwner
- **[Ext]** set_stopSellsState_oracle **#**
  - modifiers: onlyOracleManager
- **[Pub]** reflectionFromToken
- **[Pub]** tokenFromReflection
- **[Prv]** _transferBothExcluded **#**
- **[Prv]** _transferFromExcluded **#**
- **[Prv]** _transferToExcluded **#**
- **[Prv]** _transferStandard **#**
- **[Prv]** _reflectFee **#**
- **[Prv]** _getValues
- **[Prv]** _tokenTransfer **#**
- **[Prv]** _getTValues
- **[Prv]** _getRValues
- **[Prv]** _getRate
- **[Prv]** _getCurrentSupply
- **[Prv]** _takeLiquidity **#**
- **[Prv]** calculateTaxFee
- **[Prv]** calculateLiquidityFee
- **[Prv]** removeAllFee **#**
- **[Prv]** restoreAllFee **#**
- **[Prv]** swapTokensForEth **#**
- **[Prv]** swapAndLiquify **#**
- **[Prv]** transferToAddressETH **#**
- **[Prv]** _approve **#**
- **[Prv]** addLiquidity **#**
- **[Prv]** _transfer **#**
  - modifiers: ContractLock
- **[Ext]** <Fallback> **($)**

($) = 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.	Low issues
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

1. Out of gas

Issue:

- The function includeInReward() uses the loop to find and remove addresses from the _excluded list. Function will be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.

- The function _getCurrentSupply also uses the loop for evaluating total supply. It also could be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.

Recommendation:
Check that the excluded array length is not too big.

Owner privileges (In the period when the owner is not renounced)

- Owner can change _oracleManager and _presalecontract addresses.
- Owner can change presale state.
- Owner and Presale contract can add/remove addresses in special_presale_buyers.
- Owner can change swapState.
- Owner can change _oracleGasFeeAddress.
- Owner can enable/disable feesEnabled.
- Owner can change the tax, penalty and liquidity fees.
- Owner can include addresses in automatedMarketMakerPairs array.
- Owner can blacklist addresses.
- Owner can lock the contract (disable transfer function).
- Owner can withdraw contract BNBs and BEP20 tokens.
- Owner and Oracle manager can change stopSellsState.
- Owner can change the maximum transaction amount.
- Owner can exclude from the fee.
- Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.

Conclusion

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

Liquidity locking details provided by the team:
https://dx.app/app/v3/defipresale?saleID=2237&chain=BSC

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.