Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

July, 2021

Audit Details

Audited project

Daddy Reborn

Deployer address

0x99E43b35B78E2C7b175e431b566d5F53Db38E658

Client contacts:

Daddy Reborn team

Blockchain

Binance Smart Chain

Project website:

Not provided

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 Daddy Reborn to perform an audit of smart contracts:

https://bscscan.com/address/0x273bc25df2cafb50a23763f3190fa412a535eff2#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

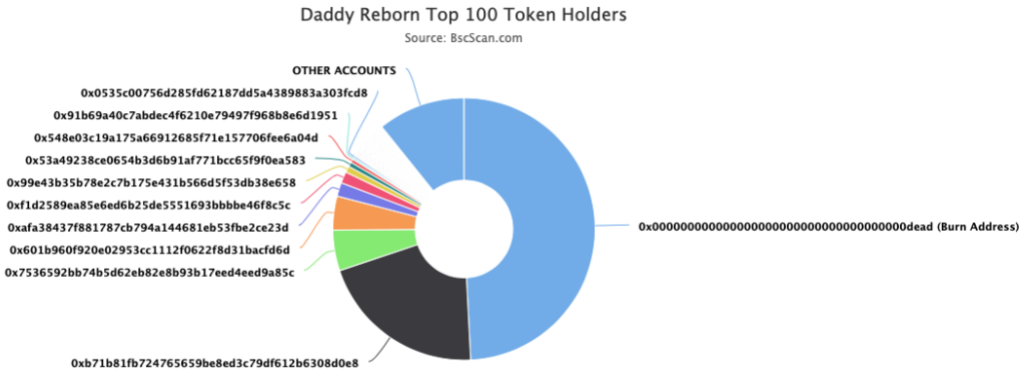
Token contract details for 17.07.2021

Contract name	Daddy Reborn
Contract address	0x273BC25dF2cafB50A23763F3190fa412A535eFF2
Total supply	1,000,000,000
Token ticker	PHNX
Decimals	9
Token holders	1,247
Transactions count	6,963
Top 100 holders dominance	89.21%
Cooldown interval	60
Autoliquidity fee receiver	0x000000000000000000000000000000000000dead
Marketing fee receiver	0xf1d2589ea85e6ed6b25de5551693bbbbe46f8c5c
Pair	0xb71b81fb724765659be8ed3c79df612b6308d0e8
Contract deployer address	0x99E43b35B78E2C7b175e431b566d5F53Db38E658
Contract's current owner address	0x99e43b35b78e2c7b175e431b566d5f53db38e658

Daddy Reborn Token Distribution

The top 100 holders collectively own 89.21% (892,118,866.09 Tokens) of Daddy Reborn

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 1,247

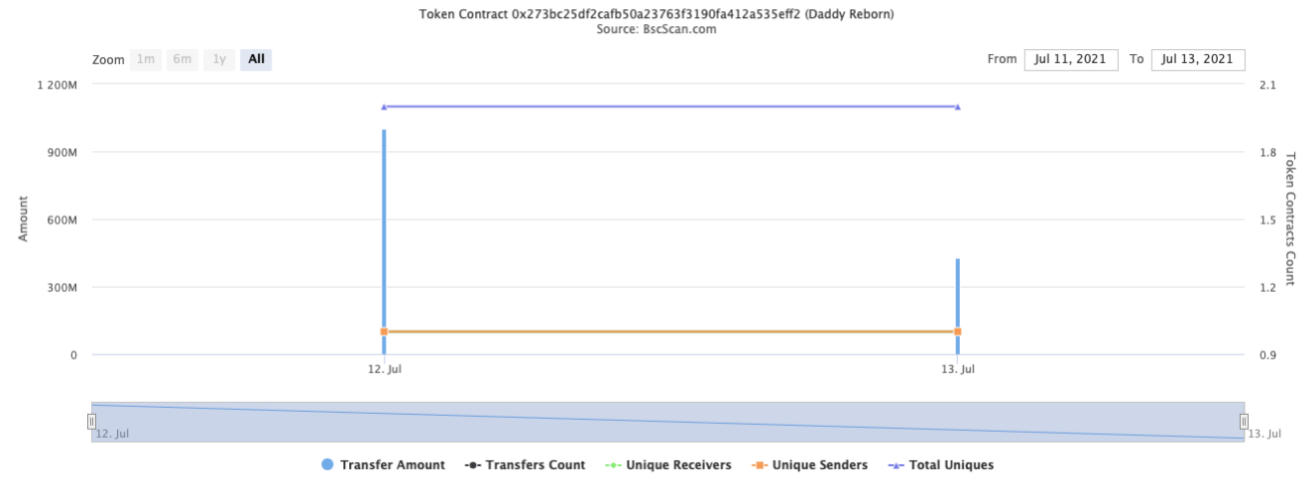


(A total of 892,118,866.09 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

Daddy Reborn Contract Interaction Details

Time Series: Token Contract Overview

Mon 12, Jul 2021 - Tue 13, Jul 2021



Daddy Reborn Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	491,935,999	49.1936%
2	0xb71b81fb724765659be8ed3c79df612b6308d0e8	206,779,968.155283853	20.6780%
3	0x7536592bb74b5d62eb82e8b93b17eed4eed9a85c	50,000,000	5.0000%
4	0x601b960f920e02953cc1112f0622f8d31bacfd6d	41,767,522.6	4.1768%
5	0xafa38437f881787cb794a144681eb53fbe2ce23d	16,799,930.88	1.6800%
6	0xf1d2589ea85e6ed6b25de5551693bbbbe46f8c5c	14,220,057.108691674	1.4220%
7	0x99e43b35b78e2c7b175e431b566d5f53db38e658	7,814,400	0.7814%
8	0x53a49238ce0654b3d6b91af771bcc65f9f0ea583	5,745,292.22	0.5745%
9	0x548e03c19a175a66912685f71e157706fee6a04d	4,199,982.72	0.4200%
10	0x91b69a40c7abdec4f6210e79497f968b8e6d1951	2,382,114.239046903	0.2382%

Contract functions details

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

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ Auth
  - [Pub] <Constructor> #
  - [Pub] authorize #
    - modifiers: onlyOwner
  - [Pub] unauthorize #
    - modifiers: onlyOwner
  - [Pub] isOwner
  - [Pub] isAuthorized
  - [Pub] transferOwnership #
    - modifiers: onlyOwner

+ [Int] IDEXFactory
  - [Ext] createPair #

+ [Int] IDEXRouter
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] IDividendDistributor
  - [Ext] setDistributionCriteria #
  - [Ext] setShare #
  - [Ext] deposit ($)
  - [Ext] process #

+ DividendDistributor (IDividendDistributor)
  - [Pub] <Constructor> #

- [Ext] setDistributionCriteria #
  - modifiers: onlyToken
- [Ext] setShare #
  - modifiers: onlyToken
- [Ext] deposit ($)
  - modifiers: onlyToken
- [Ext] process #
  - modifiers: onlyToken
- [Int] shouldDistribute
- [Int] distributeDividend #
- [Ext] claimDividend #
- [Pub] getUnpaidEarnings
- [Int] getCumulativeDividends
- [Int] addShareholder #
- [Int] removeShareholder #

+ Phoenix (IBEP20, Auth)
- [Pub] <Constructor> #
  - modifiers: Auth
- [Ext] <Fallback> ($)
- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Pub] balanceOf
- [Ext] allowance
- [Pub] approve #
- [Ext] approveMax #
- [Ext] transfer #
- [Ext] transferFrom #
- [Int] _transferFrom #
- [Int] _basicTransfer #
- [Int] checkTxLimit
- [Int] shouldTakeFee
- [Pub] getTotalFee
- [Pub] getMultipliedFee
- [Int] takeFee #
- [Int] shouldSwapBack
- [Ext] clearStuckBalance #
  - modifiers: onlyOwner
- [Pub] tradingStatus #
  - modifiers: onlyOwner
- [Pub] cooldownEnabled #
  - modifiers: onlyOwner
- [Int] swapBack #
  - modifiers: swapping
- [Int] shouldAutoBuyback
- [Ext] triggerZeusBuyback #
  - modifiers: authorized
- [Ext] clearBuybackMultiplier #
  - modifiers: authorized
- [Int] triggerAutoBuyback #
- [Int] buyTokens #
  - modifiers: swapping

- [Ext] setAutoBuybackSettings #
  - modifiers: authorized
- [Ext] setBuybackMultiplierSettings #
  - modifiers: authorized
- [Ext] keepBuybackSimple #
  - modifiers: authorized
- [Int] launched
- [Int] launch #
- [Ext] setTxLimit #
  - modifiers: authorized
- [Ext] setIsDividendExempt #
  - modifiers: authorized
- [Ext] setIsFeeExempt #
  - modifiers: authorized
- [Ext] setIsTxLimitExempt #
  - modifiers: authorized
- [Ext] setIsTimelockExempt #
  - modifiers: authorized
- [Ext] setFees #
  - modifiers: authorized
- [Ext] setFeeReceivers #
  - modifiers: authorized
- [Ext] setSwapBackSettings #
  - modifiers: authorized
- [Ext] setTargetLiquidity #
  - modifiers: authorized
- [Ext] setDistributionCriteria #
  - modifiers: authorized
- [Ext] setDistributorSettings #
  - modifiers: authorized
- [Pub] getCirculatingSupply
- [Pub] getLiquidityBacking
- [Pub] isOverLiquified
- [Ext] makeItRain #
  - modifiers: onlyOwner

($) = 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 `makeItRain()` uses the loop to airdrop rewords by the list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long receivers list.

```
ftrace | funcSig
function makeItRain(
    address from⬆,
    address[] calldata addresses⬆,
    uint256[] calldata tokens⬆
) external onlyOwner {
    uint256 showerCapacity = 0;

    require(
        addresses⬆.length == tokens⬆.length,
        "Mismatch between Address and token count"
    );

    for (uint256 i = 0; i < addresses⬆.length; i++) {
        showerCapacity = showerCapacity + tokens⬆[i];
    }

    require(
        balanceOf(msg.sender) >= showerCapacity,
        "Not enough tokens to airdrop"
    );

    for (uint256 i = 0; i < addresses⬆.length; i++) {
        _basicTransfer(from⬆, addresses⬆[i], tokens⬆[i]);
    }
}
```

Recommendation:

Check that the array length is not too big.

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

- Owner can call triggerZeusBuyback that’s initiate buyback.
- Owner can clean buyback multiplier.
- Owner can change auto buyback settings.
- Owner can change buyback multiplier settings.
- Owner can change the maximum transaction amount.
- Owner can include in and exclude from dividends.
- Owner can include in and exclude from fee and transaction amount.
- Owner can change fees.
- Owner can change fee receivers.
- Owner can change swap threshold and disable/enable swap.
- Owner can change target liquidity values.
- Owner can change distribution criteria.
- Owner can change distribution GAS.
- Owner can withdraw BNBs to the marketing receiver address.
- Owner can change trading status.
- Owner can change cooldown status.
- Owner can change buybackKeepItSimple value.
- Owner can change addresses’ isTimelockExempt value.

Conclusion

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

Liquidity locking details NOT provided by the team.

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.