Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

November, 2021

Audit Details

Audited project

SPAY

Deployer address

0xb73d7e1e3de444d6f83a1bef51478c8d30d2acbe

Client contacts:

SPAY team

Blockchain

Binance Smart Chain

Project website:

https://spay.finance/

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 SPAY to perform an audit of smart contracts:

https://bscscan.com/address/0xb21225f833f2fb1be7d88ee5347aae001f5b5db1#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 05.11.2021

Contract name	SPAY
Contract address	0xb21225F833f2Fb1BE7d88Ee5347aae001F5b5DB1
Total supply	1,000,000,000,000
Token ticker	SPAY
Decimals	9
Token holders	5,668
Transactions count	56,761
Top 100 holders dominance	64.54%
Liquidity fee	2
BNB reward fee (B/S)	9/5
Dev fee	5
Liquidity wallet	0xb73d7e1e3de444d6f83a1bef51478c8d30d2acbe
Dividend tracker	0x9d95f09a34127b8fc1977fe85b3686ff36448cb7
Uniswap V2 pair	0xec53cd7c375bb0191d4a5c0aa76739582bcd7eb1
Contract deployer address	0xb73d7e1e3de444d6f83a1bef51478c8d30d2acbe
Contract’s current owner address	0xb73d7e1e3de444d6f83a1bef51478c8d30d2acbe

SPAY Token Distribution

The top 100 holders collectively own 64.54% (645,444,673,234.81 Tokens) of SPAY

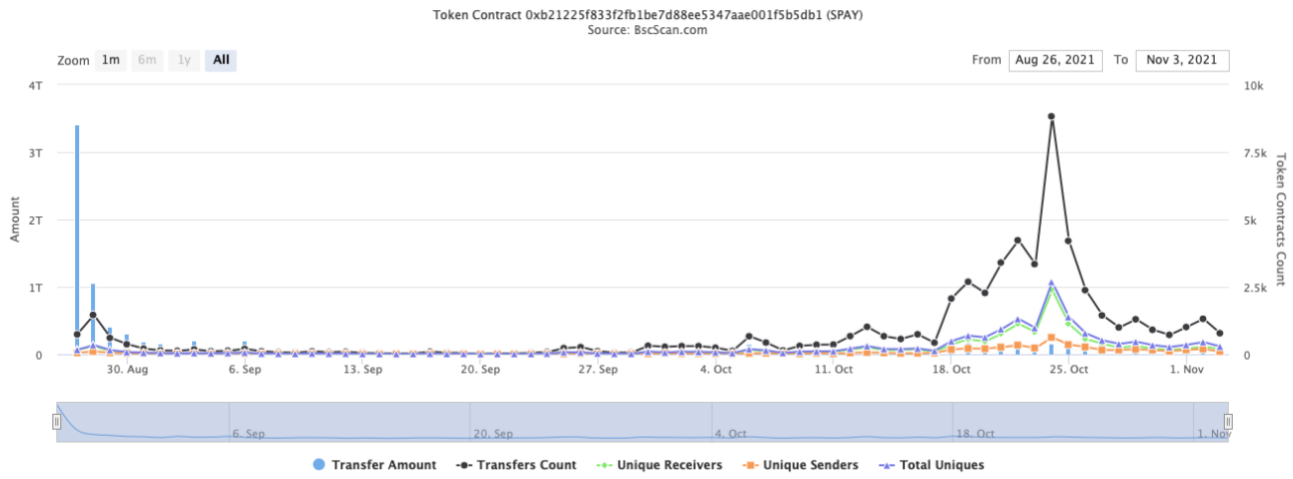
Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 5,669

(A total of 645,444,673,234.81 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

SPAY Contract Interaction Details

Time Series: Token Contract Overview

Fri 27, Aug 2021 - Wed 3, Nov 2021



SPAY Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	70,000,000,000	7.0000%
2	PancakeSwap V2: SPAY 13	46,863,538,528.803022338	4.6864%
3	0x64e6ed7ebcc3ce48961aef67086a15605ec724bd	34,683,339,094.392281356	3.4683%
4	0xccdd8a3e550d2015aef252ee03c6d89591a568d0	20,318,076,786	2.0318%
5	0xb5f7ef3c4375c6b9e8117a47a4e2f91564339c23	14,099,869,165.521099631	1.4100%
6	0x0658987dcd0171d3fc0addc79f7080684facbfd7	13,755,740,000	1.3756%
7	0x36af13e2188bcf041250231df380b828bf43aed2	12,135,871,035.736450982	1.2136%
8	0xfae4519728438afc5943856b13f88fec87333cd2	11,800,000,000	1.1800%
9	0x729c567be576763abbba24d2c20e1dd68588b51f	10,920,000,000	1.0920%
10	0xf08ae27b3b1c31d1cfc2879e2ae567d81d42bdeb	10,383,954,064.65	1.0384%

Contract functions details

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

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

+ [Lib] IterableMapping
  - [Int] get
  - [Int] getIndexOfKey
  - [Int] getKeyAtIndex
  - [Int] size
  - [Int] set #
  - [Int] remove #

```
+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Int] IERC20Metadata (IERC20)
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals

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

+ [Int] DividendPayingTokenOptionalInterface
  - [Ext] withdrawableDividendOf
  - [Ext] withdrawnDividendOf
  - [Ext] accumulativeDividendOf

+ [Int] DividendPayingTokenInterface
  - [Ext] dividendOf
  - [Ext] distributeDividends ($)
  - [Ext] withdrawDividend #

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

+  Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
```

```
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner

+ [Lib] SafeMathInt
  - [Int] mul
  - [Int] div
  - [Int] sub
  - [Int] add
  - [Int] abs
  - [Int] toUint256Safe

+ [Lib] SafeMathUint
  - [Int] toInt256Safe

+ [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 #

+  DividendPayingToken (ERC20, DividendPayingTokenInterface,
DividendPayingTokenOptionalInterface)
  - [Pub] <Constructor> #
    - modifiers: ERC20
  - [Ext] <Fallback> ($)
  - [Pub] distributeDividends ($)
  - [Pub] withdrawDividend #
  - [Int] _withdrawDividendOfUser #
  - [Pub] dividendOf
  - [Pub] withdrawableDividendOf
  - [Pub] withdrawnDividendOf
```

- [Pub] accumulativeDividendOf
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _setBalance #

+ SPAY (ERC20, Ownable)
- [Pub] <Constructor> #
  - modifiers: ERC20
- [Pub] decimals
- [Ext] <Fallback> ($)
- [Pub] updateStakingAmounts #
  - modifiers: onlyOwner
- [Ext] enableTrading #
  - modifiers: onlyOwner
- [Ext] setPresaleWallet #
  - modifiers: onlyOwner
- [Pub] enableStaking #
  - modifiers: onlyOwner
- [Pub] stake #
- [Pub] updateMaxWallet #
  - modifiers: onlyOwner
- [Pub] startBlockSniper #
  - modifiers: onlyOwner
- [Pub] stopBlockSniper #
  - modifiers: onlyOwner
- [Pub] startKillSnipe #
  - modifiers: onlyOwner
- [Pub] stopKillSnipe #
  - modifiers: onlyOwner
- [Pub] startKillPermanentSnipe #
  - modifiers: onlyOwner
- [Pub] stopKillPermanentSnipe #
  - modifiers: onlyOwner
- [Pub] updateSwapTokenAtAmount #
  - modifiers: onlyOwner
- [Pub] updateBuyAmount #
  - modifiers: onlyOwner
- [Pub] updateMaxSellAmount #
  - modifiers: onlyOwner
- [Pub] updateMaxSellAmount2 #
  - modifiers: onlyOwner
- [Pub] updateDividendTracker #
  - modifiers: onlyOwner
- [Pub] updateOperations1Address #
  - modifiers: onlyOwner
- [Pub] updateOperations2Address #
  - modifiers: onlyOwner
- [Pub] updateUniswapV2Router #
  - modifiers: onlyOwner
- [Pub] excludeFromFees #
  - modifiers: onlyOwner
- [Pub] excludeMultipleAccountsFromFees #
  - modifiers: onlyOwner
- [Pub] excludeFromSnipe #

  - modifiers: onlyOwner
- [Pub] forceConsiderAsSnipe #
- [Pub] excludeMultipleAccountsFromSnipe #
  - modifiers: onlyOwner
- [Pub] enableSwapAndLiquify #
  - modifiers: onlyOwner
- [Pub] setAutomatedMarketMakerPair #
  - modifiers: onlyOwner
- [Pub] setAllowCustomTokens #
  - modifiers: onlyOwner
- [Pub] setAllowAutoReinvest #
  - modifiers: onlyOwner
- [Prv] _setAutomatedMarketMakerPair #
- [Pub] updateLiquidityWallet #
  - modifiers: onlyOwner
- [Pub] updateGasForProcessing #
  - modifiers: onlyOwner
- [Pub] updateBNBRewardsSell #
  - modifiers: onlyOwner
- [Pub] updatesnipeBNBRewardsSell #
  - modifiers: onlyOwner
- [Pub] updatesnipeBNBRewardsBuy #
  - modifiers: onlyOwner
- [Pub] updateFees #
  - modifiers: onlyOwner
- [Ext] getStakingInfo
- [Ext] getTotalDividendsDistributed
- [Pub] isExcludedFromFees
- [Pub] isExcludedFromSnipe
- [Pub] isConsiderAsSnipe
- [Pub] withdrawableDividendOf
- [Pub] dividendTokenBalanceOf
- [Ext] getAccountDividendsInfo
- [Ext] getAccountDividendsInfoAtIndex
- [Ext] processDividendTracker #
- [Ext] claim #
- [Ext] getLastProcessedIndex
- [Ext] getNumberOfDividendTokenHolders
- [Ext] setAutoClaim #
- [Ext] setReinvest #
- [Ext] setDividendsPaused #
  - modifiers: onlyOwner
- [Ext] isExcludedFromAutoClaim
- [Ext] isReinvest
- [Int] _transfer #
- [Prv] getStakingBalance
- [Prv] swapAndLiquify #
- [Prv] swapTokensForEth #
- [Pub] updatePayoutToken #
- [Pub] getPayoutToken
- [Pub] updateAllowTokens #
  - modifiers: onlyOwner
- [Pub] getAllowTokens
- [Prv] addLiquidity #
- [Pub] forceSwapAndSendDividends #

```
    - modifiers: onlyOwner
  - [Prv] swapAndSendDividends #

+  SPAYDividendTracker (DividendPayingToken, Ownable)
  - [Pub] <Constructor> #
    - modifiers: DividendPayingToken
  - [Pub] decimals
  - [Int] _transfer
  - [Pub] withdrawDividend
  - [Ext] isExcludedFromAutoClaim
    - modifiers: onlyOwner
  - [Ext] isReinvest
    - modifiers: onlyOwner
  - [Ext] setAllowCustomTokens #
    - modifiers: onlyOwner
  - [Ext] setAllowAutoReinvest #
    - modifiers: onlyOwner
  - [Ext] excludeFromDividends #
    - modifiers: onlyOwner
  - [Ext] setAutoClaim #
    - modifiers: onlyOwner
  - [Ext] setReinvest #
    - modifiers: onlyOwner
  - [Ext] setDividendsPaused #
    - modifiers: onlyOwner
  - [Ext] getLastProcessedIndex
  - [Ext] getNumberOfTokenHolders
  - [Pub] getAccount
  - [Pub] getAccountAtIndex
  - [Ext] setBalance #
    - modifiers: onlyOwner
  - [Pub] process #
  - [Pub] processAccount #
    - modifiers: onlyOwner
  - [Pub] updateUniswapV2Router #
    - modifiers: onlyOwner
  - [Pub] updatePayoutToken #
    - modifiers: onlyOwner
  - [Pub] getPayoutToken
  - [Pub] updateAllowTokens #
    - modifiers: onlyOwner
  - [Pub] getAllowTokens
  - [Prv] _reinvestDividendOfUser #
  - [Int] _withdrawDividendOfUser #


($) = 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.	High issue
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

1. Access rights

Issue:

- The function forceConsiderAsSnipe() has only public access modifier without onlyOwner. So anybody can call this function.

Recommendation:
Be careful about including in sensitive arrays.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

2. Out of gas

Issue:

- The function excludeMultipleAccountsFromFees() uses the loop to exclude multiple accounts from fees. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.
- The function excludeMultipleAccountsFromSnipe() uses the loop to exclude multiple accounts from snipe. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.

Recommendation:
Be careful about accounts array length.

Notes:

- Dividend tracker may be changed. So that logic of setBalance and other functions could be another and not audited.
- Staking bonus automatically removes only in transferring method.
- When user reinvests tokens, automatic process is true but allowAutoReinvest is false contract will not charge dividends.
- If user not staking rewards will not charge.

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

- Owner can change staking bonus for duration.
- Owner can enable trading.
- Owner can add addresses in multiple exclusions.
- Owner can enable/disable staking.
- Owner can change max wallet token.
- Owner can start/stop block/kill snipers.
- Owner can enable/disable killPermanentSnipeEnabled.
- Owner can change swapTokensAtAmount and maxSellTransactionAmount for buy and sell.
- Owner can change dividend tracker.
- Owner can change operations 1 and 2 addresses.
- Owner can change Uniswap router address.
- Owner can exclude from the fees and snipe.
- Owner can enable/disable swap and liquify.
- Owner can exclude and include addresses in automatedMarketMakerPairs array.
- Owner can allow custom tokens and allow reinvest.
- Owner can change liquidity wallet.
- Owner can change gas for processing.
- Owner can change fees.
- Owner can pause dividends.
- Owner can change allow tokens.
- Owner can manually swap and set dividends.

Conclusion

Smart contracts contain high severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details are provided by the team:
https://dxsale.app/app/v3/dxlockview?id=0&add=0xb73D7E1E3DE444d6F83a1bef51478c8D30D2acbE&type=lplock&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.