



Presents

BullRun

Smart Contract Security Audit

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 ApeAudits and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (ApeAudits) owe no duty of care towards you or any other person, nor does ApeAudits 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 ApeAudits 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, ApeAudits hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against ApeAudits, 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.

The Ape Audits Auditors received the BRUN(BullRun)'s team application for smart contract security of the BRUN token on May 27th of 2021. The following are the details and results of this smart contract security audit:

Token Name:

BRUN

The Contract Address:

0x13D08A619848019f16F9f16D7f4b7Eb90db38Ed5

BSC Link:

<https://bscscan.com/token/0x13D08A619848019f16F9f16D7f4b7Eb90db38Ed5>

The Audit CheckList and Results:

| NO. | Audit Items | Audit Subclass | Audit Subclass Result |
|-----|-------------------------|--|--|
| 1 | Overflow Audit. | N/A | Passed |
| 2 | Race Conditions Audit | N/A | Passed |
| 3 | Authority Control Audit | Permission Vulnerability Audit Excessive Auditing Authority | Passed Passed |
| 4 | Safe Design Audit | Zeppelin Module Safe Compiler Version Hard-Coded Version Fallback Function Safeuse Show Coding Security Function Return Value Security Call Function Security. | Passed Passed Passed Passed Passed Passed |

| NO. | Audit Items | Audit Subclass | Audit Subclass Result |
|-----|--------------------------------------|----------------|-----------------------------|
| 5 | Denial of Service Audit | N/A | Passed |
| 6 | Gas Optimization Audit | N/A | Passed |
| 7 | Design Logic Audit | N/A | Passed |
| 8 | Malicious Event Log Audit | N/A | Passed(Low-security Issues) |
| 9 | “False Deposit” Vulnerability Audit | N/A | Passed |
| 10 | Uninitialized Storage Pointers Audit | N/A | Passed |
| 11 | Arithmetic Accuracy Deviation Audit | N/A | Passed |

Audit Result: Passed

Audit Date: May 27th of 2021

Audit Team: Ape Audits Auditors Team

Smart Contract Function Details

+ Bullrun (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] setUniswapPair
- [Pub] setBotPro
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Priv] TransferBothExcluded
- [Priv] TransfertoVault
- [Priv] reflectFee
- [Priv] getValues
- [Priv] getTValues
- [Priv] getRvalues
- [Priv] getRate
- [Priv] getCurrentSupply
- [Priv] takeLiquidity
- [Priv] calculateTaxFee
- [Priv] calculateLiquidityFee
- [Int] addGuardTax
- [Pub] setMaxTransactionpercent
- [Pub} setGaurdTax
- [Pub] blackListAddress
- [Priv] removeAllFee
- [Priv] restoreAllFee

-[Pub] isExcludedFromFee

-[Priv] swapandLiquify

-[Priv] swapTokensforEth

-[Priv] addLiquidity

-[Priv] transferStandard

-[Priv] transferfromExcluded

Security Issues:

High Severity Issues:

None Found.

Medium Severity Issues:

None Found.

Low Severity Issues:

- Line 717: line is redundant. Effectively the same operation is being performed in line 714.

```
_isExcludedFromFee[memeCoinManager] = true;  
    _isExcludedFromFee[devAddress] = true;  
    _isExcludedFromFee[address(this)] = true;  
    _isExcludedFromFee[msg.sender] = true;
```

- Line 733, 857-870: Bad styling. Left out commented code.

```
/*  
    function setTaxFeePercent(uint256 taxFee) external onlyMemeCoinManager() {  
        _taxFee = taxFee;  
    }  
  
    function setLiquidityFeePercent(uint256 liquidityFee) external  
onlyMemeCoinManager() {  
        _liquidityFee = liquidityFee;  
    }  
  
    function setSwapAndLiquifyEnabled(bool _enabled) public  
onlyMemeCoinManager {  
        swapAndLiquifyEnabled = _enabled;  
        emit SwapAndLiquifyEnabledUpdated(_enabled);  
    }  
*/
```

- Line 955: setMaxTransactionPercent converts numbers to 10^{-6} instead of 10^{-2} (percentages, as the name would suggest). Does not impact logic due to correct usage in code.

```
function setMaxTransactionPercent(uint256 maxTxPercent) public  
onlyMemeCoinManager() {  
    _maxTxAmount = _tTotal.mul(maxTxPercent).div(  
        10**6
```

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

- Owner can blacklist any wallet from selling.
- Owner can change the maximum transaction amount.

Comments and notes:

- Lack of unit tests.
- Code refers to "ERC20" and "ETH" in multiple places while this is "BEP20" token. No impact on logic.
- We have been informed by the team that ownership will be renounced after a “few minutes of launch”
- The tax multiple for sales will be lifted after 5 minutes.

Conclusion:

Smart Contract contain low severity issues. No medium and high severity issues were detected. LP locking details not provided by team.

Ape Auditor's Remider:

Please check the disclaimer and above and note, the audit makes no statement or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mention in the report and does not include any other potential contacts by the Owner.