# NOVOS

## KYC & AUDIT.

Novos is an agency specializing in blockchain technology solutions, Audits, KYC / Doxx.

# Table of Contents

# Audit Summary

This report has been prepared for TubePlay Token on the Binance Chain network. Novos provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.

- Testing the smart contracts against both common and uncommon attack vectors.

- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.

- Assessing the codebase to ensure compliance with current best practices and industry standards.

- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.

- Thorough line-by-line manual review of the entire codebase by industry experts.

# Project Overview

| Parameter | Result |
|---|---|
| Address | 0xE5eB08cb4057a7ea976DB6679922Bc01a845dCf8 |
| Name | TubePlay |
| Token Tracker | TUBE |
| Decimals | 18 |
| Supply | 100,000,000 |
| Platform | Binance Chain |
| Compiler | v0.8.7+commit.e28d00a7 |
| Optimization | No with 200 runs |
| Other Settings: | default evmVersion, MIT license |
| Language | Solidity |
| Codebase | https://bscscan.com/address/0xE5eB08cb4057a7ea976DB6679922Bc01a845dCf8#code |
| Url | https://tube-play.com/ |

## Main Contract Assessed

| Name | Contract | Live |
|---|---|---|
| **TubePlay** | 0xE5eB08cb4057a7ea976DB6679922Bc01a845dCf8 | Yes |

# Smart Contract Vulnerability Checks

| Vulnerability | Automatic Scan | Manual Scan | Result |
|---|---|---|---|
| ❖ Unencrypted Private Data On-Chain | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Code With No Effects | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Message call with hardcoded gas amount | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Hash Collisions With Multiple Variable Length Arguments | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Unexpected Ether balance | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Presence of unused variables | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Right-To-Left-Override control character (U+202E) | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Typographical Error | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ DoS With Block Gas Limit | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Arbitrary Jump with Function Type Variable | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Insufficient Gas Griefing | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Incorrect Inheritance Order | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Write to Arbitrary Storage Location | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Requirement Violation | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Missing Protection against Signature Replay Attacks | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Weak Sources of Randomness from Chain Attributes | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |

# Smart Contract Vulnerability Checks

| Vulnerability | Automatic Scan | Manual Scan | Result |
|---|---|---|---|
| ❖ Authorization through tx.origin | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Delegatecall to Untrusted Callee | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Use of Deprecated Solidity Functions | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Assert Violation | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Reentrancy | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Unprotected SELFDESTRUCT Instruction | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Unprotected Ether Withdrawal | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Unchecked Call Return Value | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Outdated Compiler Version | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Integer Overflow and Underflow | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Function Default Visibility | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |

# Contract
# Ownership

The contract ownership of TubePlay is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

.

**01** The current owner is the address 0xeAd5b6d797053e1456450a83eB5D0D232F5EA2f4 which can be viewed from: HERE

**02** The owner wallet has the power to call the functions displayed on the priviliged functions chart below, if the owner wallet is compromised this privileges could be exploited.

**03** We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

NOVOS

**NOVOS**

# Important Notes To The Users:

**01**    The owner cannot stop trading.

**02**    The owner cannot blacklist wallets.

**03**
Constructor() ERC20("TubePlay Token", "TUBE") ListingController(100) { _mint(msg.sender, 100000000 * (10**18)); excludeFromFee(address(this)); excludeFromFee(msg.sender); uint buyFee = 0; uint sellFee = 0; uint normalFee = 0;

**04**    Owner can enable trading but cannot pause or disable it.

**05**
Require(buyFee_ <= 20, "TransferFee: fee must be less or equal 20%"); require(sellFee_ <= 20, "TransferFee: fee must be less or equal 20%"); require(normalFee_ <= 20, "TransferFee: fee must be less or equal 20%");

**06**
_allowances[sender][msg.sender] = _allowances[sender][msg.sender].sub(amount, "Insufficient Allowance");

**07**    Owner can change the claimWait for dividends between 1 hour and 24  hours.

**08**
Mapping(address => bool) private blackListedList; mapping(address => bool) private isExcludedFromFee; uint256 private maxAmount = 1000 * 10**3 * 10**18; //1% uint256 private swapTokensAtAmount = 10**3 * 10**18; STransferFee private _transferFee; uint constant private DEMI = 100;

**09**    Owner can change and configure the dividendTracker with no  constrains.

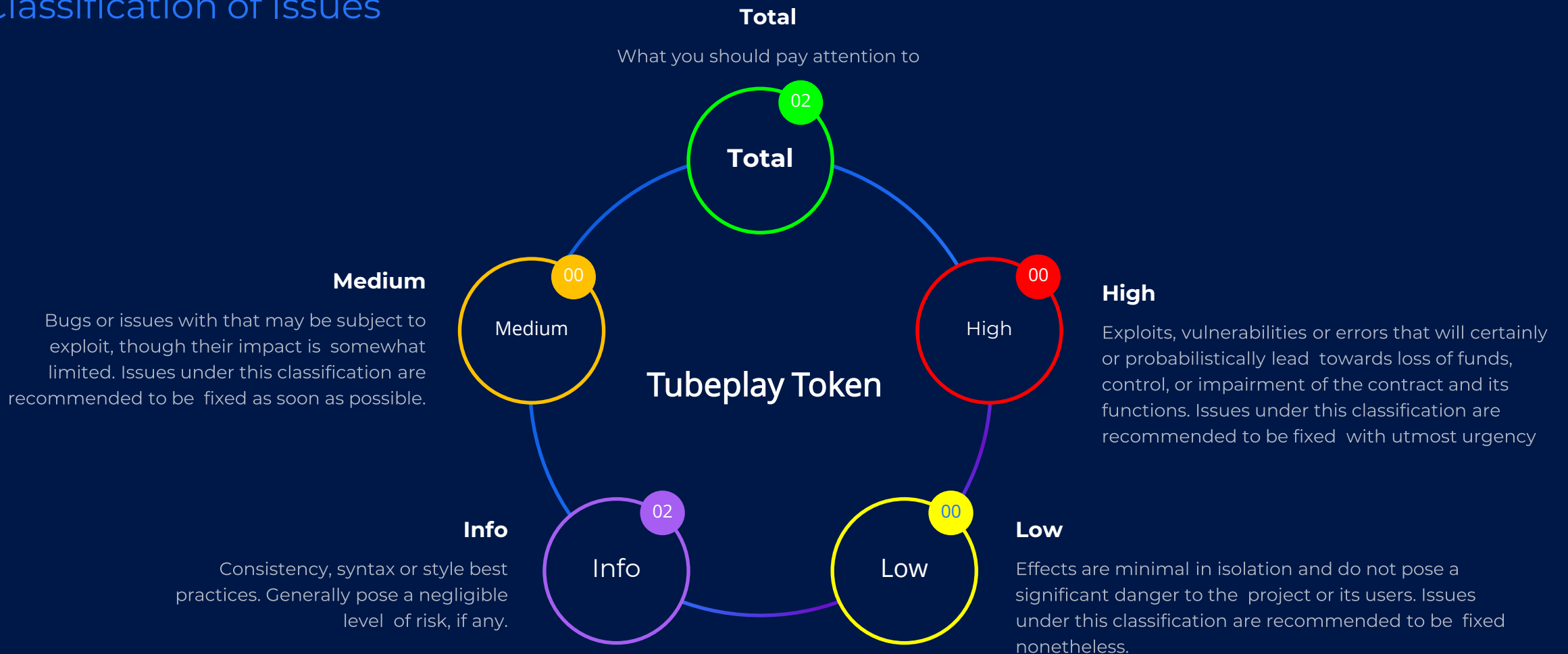**10**    swapThreshold = _totalSupply / 10000 * 42; // 0.42%.

**11**    Owner can add/remove wallets from fee exemption and dividends.

**12**    Owner can change the minimum token balance needed to get dividends.  No high-riskExploits /Vulnerabilities Were Found in token Source Code.
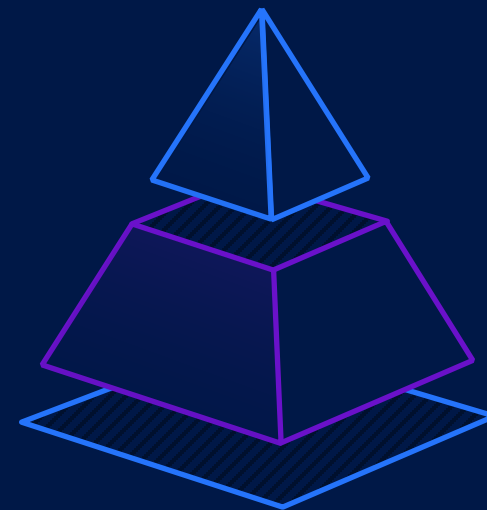
# Technical Findings Summary
## Classification of Issues

**NOVOS**

**Total**
What you should pay attention to

**02**

**Total**

**Medium**

Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.

**00**

Medium

**Tubeplay Token**

**00**

High

**High**

Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency

**Info**

Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

**02**

Info

**00**

Low

**Low**

Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.

# Findings

## Public function that could be declared external

| ID | Severity | Contract | Function |
|----|----------|----------|----------|
| 01 | Informational | Tubeplay | Functions: size, getKeyAtIndex, getIndexOfKey |

**Description**

Gas Optimization. Public function that could be declared external

**Recommendation**

Public functions that are never called by the contract should be declared external to save gas.

# Findings

## Missing events arithmetic
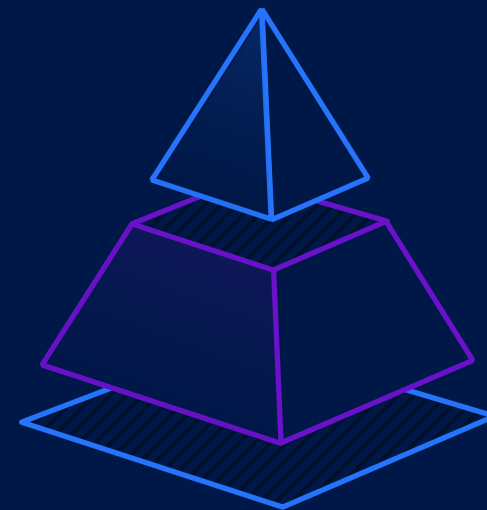
| ID | Severity | Contract | Function |
|----|----------|----------|----------|
| 02 | Informational | Tubeplay | Missing events for setWalletBalance, setMaxBuyTransaction, setMaxSellTransaction, setSwapTokensAtAmount, setSellTransactionMultiplier |

### Description

Functions that change critical arithmetic parameters should emit an event.

### Recommendation

Emit corresponding events for critical parameter changes.

# Priviliged Functions (onlyOwner & Others)

| Function Name | Parameters | Visibility |
|---|---|---|
| ✓ renounceOwnership | ▪ none | ▪ **external** |
| ✓ transferOwnership | ▪ address newOwner | ▪ **public** |
| ✓ prepareForPartherOrExchang eListing | ▪ address_partnerOrExchangeAddress | ▪ **external** |
| ✓ setWalletBalance | ▪ uint256 _maxWalletBalance | ▪ **external** |
| ✓ setMaxBuyTransaction | ▪ uint256 _maxTxn | ▪ **external** |
| ✓ setMaxSellTransaction | ▪ uint256 _maxTxn | ▪ **external** |
| ✓ updateBusdDividendToken | ▪ address _newContract | ▪ **external** |
| ✓ updateMarketingWallet | ▪ address _newWallet | ▪ **external** |
| ✓ setSwapTokensAtAmount | ▪ uint256 _swapAmount | ▪ **external** |
| ✓ setSellTransactionMultiplier | ▪ uint256 _multiplier | ▪ **external** |
| ✓ setTradingIsEnabled | ▪ none | ▪ **external** |
| ✓ setBusdDividendEnabled | ▪ bool _enabled | ▪ **external** |
| ✓ setMarketingEnabled | ▪ bool _enabled | ▪ **external** |
| ✓ setSwapAndLiquifyEnabled | ▪ bool _enabled | ▪ **external** |
| ✓ updatebusdDividendTracker | ▪ address newAddress | ▪ **external** |
| ✓ updateUniswapV2Router | ▪ address newAddress | ▪ **external** |

# Priviliged Functions (onlyOwner & Others)

| Function Name | Parameters | Visibility |
|---|---|---|
| ✓ excludeFromFees | ▪ address account, bool excluded | ▪ **public** |
| ✓ excludeFromDividend | ▪ address account | ▪ **public** |
| ✓ setAutomatedMarketMakerP air | ▪ address pair, bool value | ▪ **external** |
| ✓ updateGasForProcessing | ▪ uint256 newValue | ▪ **external** |
| ✓ updateMinimumBalanceForDi  vidends | ▪ uint256 newMinimumBalance | ▪ **external** |
| ✓ updateClaimWait | ▪ uint256 claimWait | ▪ **external** |
| ✓ processDividendTracker | ▪ uint256 gas | ▪ **external** |
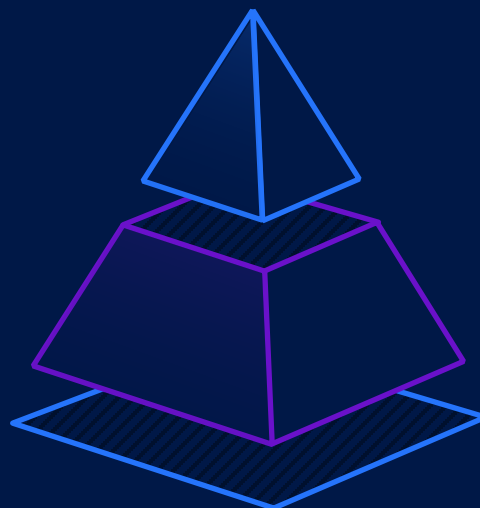
# Statistics

## Liquidity Info
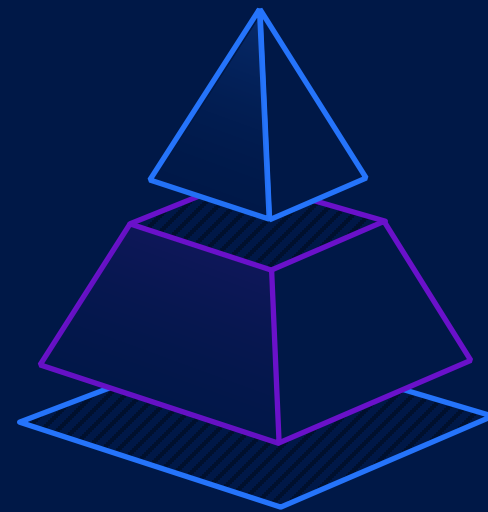
| Parameter | Result |
|---|---|
| Pair Address | 0x096c3b1003174b363c32debeea358d9d44906531 |
| Tubeplay Reserves | 0.00 TUBE |
| BNB Reserves | 0.00 BNB |
| Liquidity Value | $0 USD |

NOVOS

# Statistics

## Token (TUBE) Holders Info
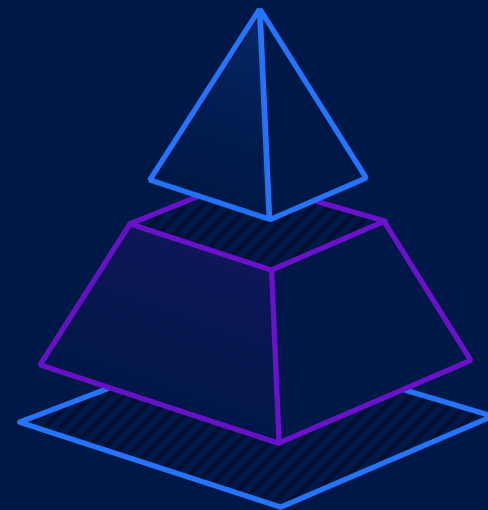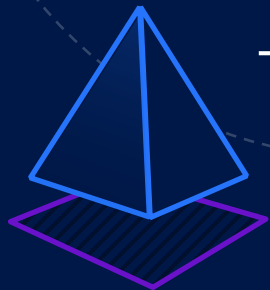
| Parameter | Result |
| --- | --- |
| Tubeplay Percentage Burnt | 0.00% |
| Tubeplay Amount Burnt | 0 TUBE |
| Top 10 Percentage Own | 100% |
| Top 10 Amount Owned | 100,000,000 TUBE |
| Top 10 Value | $NaN USD |

# Statistics

## LP (TUBE /BNB) Holders Info

| Parameter | Result |
|---|---|
| TUBE/BNB % Burnt | 0.00% |
| TUBE/BNB Amount Burnt | 0 TUBE/BNB |
| Top 10 Percentage Owned | 0.00% |
| Top 10 Amount Owned | 0 TUBE/BNB |
| Locked Tokens Percentage | 0.00% |

❖ All the data displayed above was taken on-chain at block 19488796
❖ The tokens on industry-standard burn wallets are not included on the top 10 wallets calculations

# Disclaimer