# COINSCOPE

# Audit Report

# Good Dao

December 2021

Type        BEP20

Address     0x048FFa8aAE293470932388b615A90A8265bFB25F

Audited by   © coinscope

# Table of Contents

# Contract Review

| Contract Name | GDG |
|---|---|
| Compiler Version | v0.8.4+commit.c7e474f2 |
| Optimization | 200 runs |
| Licence | Unlicense |
| Explorer | https://bscscan.com/token/0x048FFa8aAE293470932388b615A90A8265bFB25F |
| Symbol | GDG |
| Decimals | 9 |
| Total Supply | 10,000,000,000 |
| Source | contract.sol |
| Domain | |

# Audit Updates

| Initial Audit | 28th December 2021 |
|---|---|
| Corrected | |

# Contract Analysis

● Critical     ● Medium     ● Pass

| Severity | Code | Description |
|---|---|---|
| ● | MT | Contract Owner is not able to mint new tokens |
| ● | BT | Contract Owner is not able to burn tokens from specific wallet |
| ● | ELFM | Contract Owner is not able to increase fees more than a reasonable percent (25%) |
| ● | ST | Contract Owner is not able to pause transactions for everyone else except him |
| ● | OCTD | Contract Owner is not able to transfer tokens from specific address |
| ● | ULTW | Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent |
| ● | BC | Contract Owner is not able to blacklist wallets from selling |

# ELFM - Exceed Limit Fees Manipulation

| Criticality | critical |
|---|---|
| Location | https://bscscan.com/address/0x048FFa8aAE293470932388b615A90A8265bFB25F#code#L889 |

## Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the `setTaxFeePercent` function with a high percentage value.

```
function setTaxFeePercent(uint256 taxFee) external onlyOwner() {
    _taxFee = taxFee;
}
```

## Recommendation

The contract could embody a check for the maximum acceptable value.

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

# ST - Stop Transactions

| Criticality | medium |
|---|---|
| Location | https://bscscan.com/address/0x048FFa8aAE293470932388b615A90A8265bFB2 5F#code#L1015 |

## Description

The contract owner has the authority to stop transactions for all users excluding the owner. The owner may take advantage of it by setting the `_maxTxAmount` to zero.

```
    if(from != owner() && to != owner()) {
        require(amount <= _maxTxAmount, "Transfer amount exceeds the
maxTxAmount.");
    }
```

## Recommendation

The contract could embody a check for not allowing setting the _maxTxAmount less than a reasonable amount. A suggested implementation could check that the maximum amount should be more than a fixed percentage of the total supply.

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

# Contract Diagnostics

| Pass | Name |
| --- | --- |
| ✓ | Integer Underflow |
| ✓ | Parity Multisig Bug |
| ✓ | Callstack Depth Attack |
| ✓ | Transaction-Ordering Dependency |
| ✓ | Timestamp Dependency |
| ✓ | Re-Entrancy |

# Contract Functions

| Contract | Type | Bases | | |
|---|---|---|---|---|
| | Function Name | Visibility | Mutability | Modifiers |
| | | | | |
| **Context** | Implementation | | | |
| | _msgSender | Internal | | |
| | _msgData | Internal | | |
| | | | | |
| **IERC20** | Interface | | | |
| | totalSupply | External | | - |
| | balanceOf | External | | - |
| | transfer | External | ✓ | - |
| | allowance | External | | - |
| | approve | External | ✓ | - |
| | transferFrom | External | ✓ | - |
| | | | | |
| **SafeMath** | Library | | | |
| | add | Internal | | |
| | sub | Internal | | |
| | sub | Internal | | |
| | mul | Internal | | |
| | div | Internal | | |
| | div | Internal | | |
| | mod | Internal | | |
| | mod | Internal | | |
| | | | | |
| **Address** | Library | | | |
| | isContract | Internal | | |
| | sendValue | Internal | ✓ | |
| | functionCall | Internal | ✓ | |
| | functionCall | Internal | ✓ | |

| | functionCallWithValue | Internal | ✓ | |
|---|---|---|---|---|
| | functionCallWithValue | Internal | ✓ | |
| | _functionCallWithValue | Private | ✓ | |
| | | | | |
| **Ownable** | Implementation | Context | | |
| | <Constructor> | Public | ✓ | - |
| | owner | Public | | - |
| | renounceOwnership | Public | ✓ | onlyOwner |
| | transferOwnership | Public | ✓ | onlyOwner |
| | getUnlockTime | Public | | - |
| | getTime | Public | | - |
| | lock | Public | ✓ | onlyOwner |
| | unlock | Public | ✓ | - |
| | | | | |
| **IUniswapV2Factory** | Interface | | | |
| | feeTo | External | | - |
| | feeToSetter | External | | - |
| | getPair | External | | - |
| | allPairs | External | | - |
| | allPairsLength | External | | - |
| | createPair | External | ✓ | - |
| | setFeeTo | External | ✓ | - |
| | setFeeToSetter | External | ✓ | - |
| | | | | |
| **IUniswapV2Pair** | Interface | | | |
| | name | External | | - |
| | symbol | External | | - |
| | decimals | External | | - |
| | totalSupply | External | | - |
| | balanceOf | External | | - |
| | allowance | External | | - |
| | approve | External | ✓ | - |
| | transfer | External | ✓ | - |
| | transferFrom | External | ✓ | - |

| | DOMAIN_SEPARATOR | External | | - |
|---|---|---|---|---|
| | PERMIT_TYPEHASH | External | | - |
| | nonces | External | | - |
| | permit | External | ✓ | - |
| | MINIMUM_LIQUIDITY | External | | - |
| | factory | External | | - |
| | token0 | External | | - |
| | token1 | External | | - |
| | getReserves | External | | - |
| | price0CumulativeLast | External | | - |
| | price1CumulativeLast | External | | - |
| | kLast | External | | - |
| | burn | External | ✓ | - |
| | swap | External | ✓ | - |
| | skim | External | ✓ | - |
| | sync | External | ✓ | - |
| | initialize | External | ✓ | - |
| | | | | |
| **IUniswapV2Router01** | Interface | | | |
| | factory | External | | - |
| | WETH | External | | - |
| | addLiquidity | External | ✓ | - |
| | addLiquidityETH | External | Payable | - |
| | removeLiquidity | External | ✓ | - |
| | removeLiquidityETH | External | ✓ | - |
| | removeLiquidityWithPermit | External | ✓ | - |
| | removeLiquidityETHWithPermit | External | ✓ | - |
| | swapExactTokensForTokens | External | ✓ | - |
| | swapTokensForExactTokens | External | ✓ | - |
| | swapExactETHForTokens | External | Payable | - |
| | swapTokensForExactETH | External | ✓ | - |
| | swapExactTokensForETH | External | ✓ | - |
| | swapETHForExactTokens | External | Payable | - |
| | quote | External | | - |
| | getAmountOut | External | | - |

| | getAmountIn | External | | - |
|---|---|---|---|---|
| | getAmountsOut | External | | - |
| | getAmountsIn | External | | - |
| | | | | |
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 | | |
| | removeLiquidityETHSupportingFeeOnTransferTokens | External | ✓ | - |
| | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External | ✓ | - |
| | swapExactTokensForTokensSupportingFeeOnTransferTokens | External | ✓ | - |
| | swapExactETHForTokensSupportingFeeOnTransferTokens | External | Payable | - |
| | swapExactTokensForETHSupportingFeeOnTransferTokens | External | ✓ | - |
| | | | | |
| **GDG** | Implementation | Context, IERC20, Ownable | | |
| | <Constructor> | Public | ✓ | - |
| | name | Public | | - |
| | symbol | Public | | - |
| | decimals | Public | | - |
| | totalSupply | Public | | - |
| | balanceOf | Public | | - |
| | transfer | Public | ✓ | - |
| | allowance | Public | | - |
| | approve | Public | ✓ | - |
| | transferFrom | Public | ✓ | - |
| | increaseAllowance | Public | ✓ | - |
| | decreaseAllowance | Public | ✓ | - |
| | isExcludedFromReward | Public | | - |
| | totalFees | Public | | - |
| | minimumTokensBeforeSwapAmount | Public | | - |
| | buyBackUpperLimitAmount | Public | | - |
| | deliver | Public | ✓ | - |
| | reflectionFromToken | Public | | - |

| | | | | |
|---|---|---|---|---|
| | tokenFromReflection | Public | | - |
| | excludeFromReward | Public | ✓ | onlyOwner |
| | includeInReward | External | ✓ | onlyOwner |
| | _approve | Private | ✓ | |
| | _transfer | Private | ✓ | |
| | swapTokens | Private | ✓ | lockTheSwap |
| | buyBackTokens | Private | ✓ | lockTheSwap |
| | swapTokensForEth | Private | ✓ | |
| | swapETHForTokens | Private | ✓ | |
| | addLiquidity | Private | ✓ | |
| | _tokenTransfer | Private | ✓ | |
| | _transferStandard | Private | ✓ | |
| | _transferToExcluded | Private | ✓ | |
| | _transferFromExcluded | Private | ✓ | |
| | _transferBothExcluded | Private | ✓ | |
| | _reflectFee | Private | ✓ | |
| | _getValues | Private | | |
| | _getTValues | Private | | |
| | _getRValues | Private | | |
| | _getRate | Private | | |
| | _getCurrentSupply | Private | | |
| | _takeLiquidity | Private | ✓ | |
| | calculateTaxFee | Private | | |
| | calculateLiquidityFee | Private | | |
| | removeAllFee | Private | ✓ | |
| | restoreAllFee | Private | ✓ | |
| | isExcludedFromFee | Public | | - |
| | excludeFromFee | Public | ✓ | onlyOwner |
| | includeInFee | Public | ✓ | onlyOwner |
| | setTaxFeePercent | External | ✓ | onlyOwner |
| | setLiquidityFeePercent | External | ✓ | onlyOwner |
| | setMaxTxAmount | External | ✓ | onlyOwner |
| | setMarketingDivisor | External | ✓ | onlyOwner |
| | setNumTokensSellToAddToLiquidity | External | ✓ | onlyOwner |
| | setBuybackUpperLimit | External | ✓ | onlyOwner |

| | setMarketingAddress | External | ✓ | onlyOwner |
|---|---|---|---|---|
| | setSwapAndLiquifyEnabled | Public | ✓ | onlyOwner |
| | setBuyBackEnabled | Public | ✓ | onlyOwner |
| | prepareForPreSale | External | ✓ | onlyOwner |
| | afterPreSale | External | ✓ | onlyOwner |
| | transferToAddressETH | Private | ✓ | |
| | <Receive Ether> | External | Payable | - |

# Contract Flow

# Summary

Good Dao is an interesting project aiming to combine Global Philanthropy with the cryptocurrency world. The token has a friendly and growing community. There are some functions that can be abused by the owner, like manipulating fees to high values and changing max transaction amount to a very small value. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

# Disclaimer

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment.

Coinscope team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed.

The Coinscope team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Coinscope receive a payment to manipulate those results or change the awarding badge that we will be adding in our website.

Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token.

The Coinscope team disclaims any liability for the resulting losses.

# About Coinscope

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.

The Coinscope.co team

https://www.coinscope.co