Audit Report

DumbleDAO

January 2022

Type	BEP20
Network	BSC
Address	0xf942eA9174DDA116EECcBeDf71a4951E428a266E
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	DumbleDAO
Compiler Version	v0.8.0+commit.c7dfd78e
Optimization	200 runs
Licence	
Explorer	https://bscscan.com/token/0xf942eA9174DDA116EECcBeDf71a4951E428a266E
Symbol	DUMBLE
Decimals	18
Total Supply	7,777,777
Source	contracts/DumbleDAO.sol, @openzeppelin/contracts/token/ERC20/ERC20.sol, @openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol, @openzeppelin/contracts/access/AccessControl.sol, @openzeppelin/contracts/token/ERC20/IERC20.sol, @openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol, @openzeppelin/contracts/utils/Context.sol, @openzeppelin/contracts/access/IAccessControl.sol, @openzeppelin/contracts/utils/Strings.sol, @openzeppelin/contracts/utils/introspection/ERC165.sol, @openzeppelin/contracts/utils/introspection/IERC165.sol
Domain	dumbledao.io

Audit Updates

Initial Audit	20th January 2022

Corrected	

Contract Analysis

● Critical ● Medium ● Minor ● Pass

Severity	Code	Description
●	ST	Contract Owner is not able to stop or pause transactions
●	OCTD	Contract Owner is not able to transfer tokens from specific address
●	OTUT	Owner Transfer User's Tokens
●	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
●	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
●	MT	Contract Owner is not able to mint new tokens
●	BT	Contract Owner is not able to burn tokens from specific wallet
●	BC	Contract Owner is not able to blacklist wallets from selling

ELFM - Exceed Limit Fees Manipulation

Criticality	medium
Location	contract.sol#L1

Description

The contract owner has the authority to increase over the allowed limit of 25% the transaction fees of some wallets. The owner may take advantage of it by calling the `setTreasuryTax` function with a high percentage value and adding the specific wallet in the `_isTaxed` array

```
function setTreasuryTax(uint256 _tax) public virtual onlyRole(OWNER_ROLE) {
    treasuryTax = _tax;
}
```

```
if (isTaxed(sender) || isTaxed(recipient)) {
    uint256 toTreasury = (amount * treasuryTax) / DENOMINATOR;
    uint256 toTeam = (amount * teamTax) / DENOMINATOR;
    uint256 lessTax = amount - (toTreasury + toTeam);
    _transfer(sender, treasury, toTreasury);
    _transfer(sender, team, toTeam);

    return lessTax;
}
```

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.

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	L01	Public Function could be Declared External
	L04	Conformance to Solidity Naming Conventions
	L09	Dead Code Elimination

L01 - Public Function could be Declared External

Criticality	minor
Location	@openzeppelin/contracts/access/AccessControl.sol#L123,L119,L115 and 16 more

Description

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

```
setTeamTax
setTreasuryTax
setTeam
...
```

Recommendation

Use the external attribute for functions never called from the contract

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contracts/DumbleDAO.sol#L131,L123,L119 and 4 more

Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
_address
_tax
...
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions

L09 - Dead Code Elimination

Criticality	minor
Location	@openzeppelin/contracts/access/AccessControl.sol#L14,L39,L20 and 1 more

Description

Functions that are not used in the contract, and make the code's size bigger.

```
toString
toHexString
_msgData
...
```

Recommendation

Remove unused functions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
AccessControl	Implementation	Context, IAccessControl, ERC165		
	supportsInterface	Public		-
	hasRole	Public		-
	_checkRole	Internal		
	getRoleAdmin	Public		-
	grantRole	Public	✓	onlyRole
	revokeRole	Public	✓	onlyRole
	renounceRole	Public	✓	-
	_setupRole	Internal	✓	
	_setRoleAdmin	Internal	✓	
	_grantRole	Private	✓	
	_revokeRole	Private	✓	
IAccessControl	Interface			
	hasRole	External		-
	getRoleAdmin	External		-
	grantRole	External	✓	-
	revokeRole	External	✓	-
	renounceRole	External	✓	-
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-

	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
ERC20Burnable	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Context	Implementation			

	_msgSender	Internal		
	_msgData	Internal		
ERC165	Implementation	IERC165		
	supportsInterface	Public		-
IERC165	Interface			
	supportsInterface	External		-
Strings	Library			
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
DumbleDAO	Implementation	ERC20, ERC20Burnable, AccessControl		
	<Constructor>	Public	✓	ERC20
	addTaxed	Public	✓	onlyRole
	removeTaxed	Public	✓	onlyRole
	setTreasury	Public	✓	onlyRole
	setTeam	Public	✓	onlyRole
	setTreasuryTax	Public	✓	onlyRole
	setTeamTax	Public	✓	onlyRole
	isTaxed	Public		-
	_taxed	Internal	✓	
	_taxTransfer	Internal	✓	
	transfer	Public	✓	-
	transferFrom	Public	✓	-

Contract Flow

Domain Info

Domain Name	dumbledao.io
Registry Domain ID	dda40805e8474b21a35b9c8f239bc98a-DONUTS
Creation Date	2022-01-01T06:24:32Z
Updated Date	2022-01-06T06:25:24Z
Registry Expiry Date	2023-01-01T06:24:32Z
Registrar WHOIS Server	whois.godaddy.com/
Registrar URL	http://www.godaddy.com/domains/search.aspx?ci=8990
Registrar	GoDaddy.com, LLC
Registrar IANA ID	146

The domain has been created 19 days before the creation of the audit. It will expire in 12 months.

There is no public billing information, the creator is protected by the privacy settings.

Summary

The Smart Contract analysis reported one issue. The contract owner has the ability to increase the fees from specific wallets more than the maximum allowed limit. 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