Cyberscope

Audit Report

SunDAO

August 2022

Type	BEP20
Network	BSC
Address	0x75630b69ba8520e177a5653ca886cef84f43adc3
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	SunDAO
Compiler Version	v0.6.12+commit.27d51765
Optimization	200 runs
Licence	
Explorer	https://bscscan.com/token/0x75630b69ba8520e177a5653ca886cef84f43adc3
Symbol	SDAO
Decimals	9
Total Supply	10,000,000,000
Domain	sundao.finance

Audit Updates

Initial Audit	6th August 2022
Corrected	

Source Files

Filename	**SHA256**
@openzeppelin/contracts/access/Ownable.sol	b9f957b42bdcf3d3499be4c94558152e91658e34a1fe5a5e8f0972ce20e15ed7
@openzeppelin/contracts/math/SafeMath.sol	4a04d0a20a19e3ef1dcabae9cad9ba006430a4e7eec4d9b519db87999722c98a

@openzeppelin/contracts/token/ERC20/IERC20.sol	0573c2961569aa4906845d0cd428b5b7394956170054ceeaa8f8af96cd44875c
@openzeppelin/contracts/utils/Address.sol	11ad5e3e21434e00c4ceba1f5a977b7a68bdd7d16b849276ce4ff4495129eec7
@openzeppelin/contracts/utils/Context.sol	9a3d1e5be0f0ace13e2d9aa1d0a1c3a6574983983ad5de94fc412f878bf7fe89
contracts/token/SunDAO.sol	c3916e5129588160862c36d423540bc3650c903983b37b8cf8ae80ff8641667d

The Smart Contract interacts with an external contract who’s code is not visible hence is not within the scope of the Audit.

Disclaimer: This can be a simple bot protection, or a very malicious honeypot functionality; there is no way for the auditor to know the context of the source. Do your Own research and check more info on the Untrusted Source Section

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

ULTW - Unlimited Liquidity to Team Wallet

Criticality	minor
Location	contract.sol#L337

Description

The contract owner has the authority to transfer funds without limit to the team wallet. These funds have been accumulated from fees collected from the contract. The owner may take advantage of it by calling the `manualSend` method/

```
function manualSend() external onlyGovernor {
   sendETHToFee(address(this).balance);
 }
```

Recommendation

The contract could embody a check for the maximum amount of funds that can be swapped. Since a huge amount may volatile the token's price.

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
	US	Untrusted Source
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L04	Conformance to Solidity Naming Conventions
	L05	Unused State Variable
	L09	Dead Code Elimination

US - Untrusted Source

Criticality	critical
Location	contract.sol#L362

Description

The contract uses an external contract in order to determine the transaction's flow. The external contract is untrusted. As a result it may produce security issues and harm the transactions.

```
if (bpEnabled) {
     bp.protect(from, to, amount);
   }
```

Recommendation

The contract should use a trusted external source. A trusted source could be either a commonly recognized or an audited contract. The pointing addresses should not be able to change after the initialization.

L01 - Public Function could be Declared External

Criticality	minor
Location	@openzeppelin/contracts/access/Ownable.sol#L54,63 contracts/token/SunDAO.sol#L104,108,112,116,124,129,133,138,152,341,347,353

Description

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

```
setNewMarketingAddress
setNewDevelopmentAddress
excludeMultipleAccountsFromFees
totalFees
transferFrom
approve
allowance
transfer
totalSupply
...
```

Recommendation

Use the external attribute for functions never called from the contract.

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contracts/token/SunDAO.sol#L61,59,60,46,52,50,51,54

Description

Constant state variables should be declared constant to save gas.

```
taxFee
marketingFee
developmentFee
burnFee
_tTotal
_symbol
_name
_decimals
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contracts/token/SunDAO.sol#L24,362,366

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.

```
_enabled
_bp
WETH
```

Recommendation

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

L05 - Unused State Variable

Criticality	minor
Location	contracts/token/SunDAO.sol#L40

Description

There are segments that contain unused state variables.

```
_tOwned
```

Recommendation

Remove unused state variables.

L09 - Dead Code Elimination

Criticality	minor
Location	@openzeppelin/contracts/utils/Address.sol#L171,79,89,104,114,153,163,129,139,26,53

Description

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

```
sendValue
isContract
functionStaticCall
functionDelegateCall
functionCallWithValue
functionCall
_verifyCallResult
...
```

Recommendation

Remove unused functions.

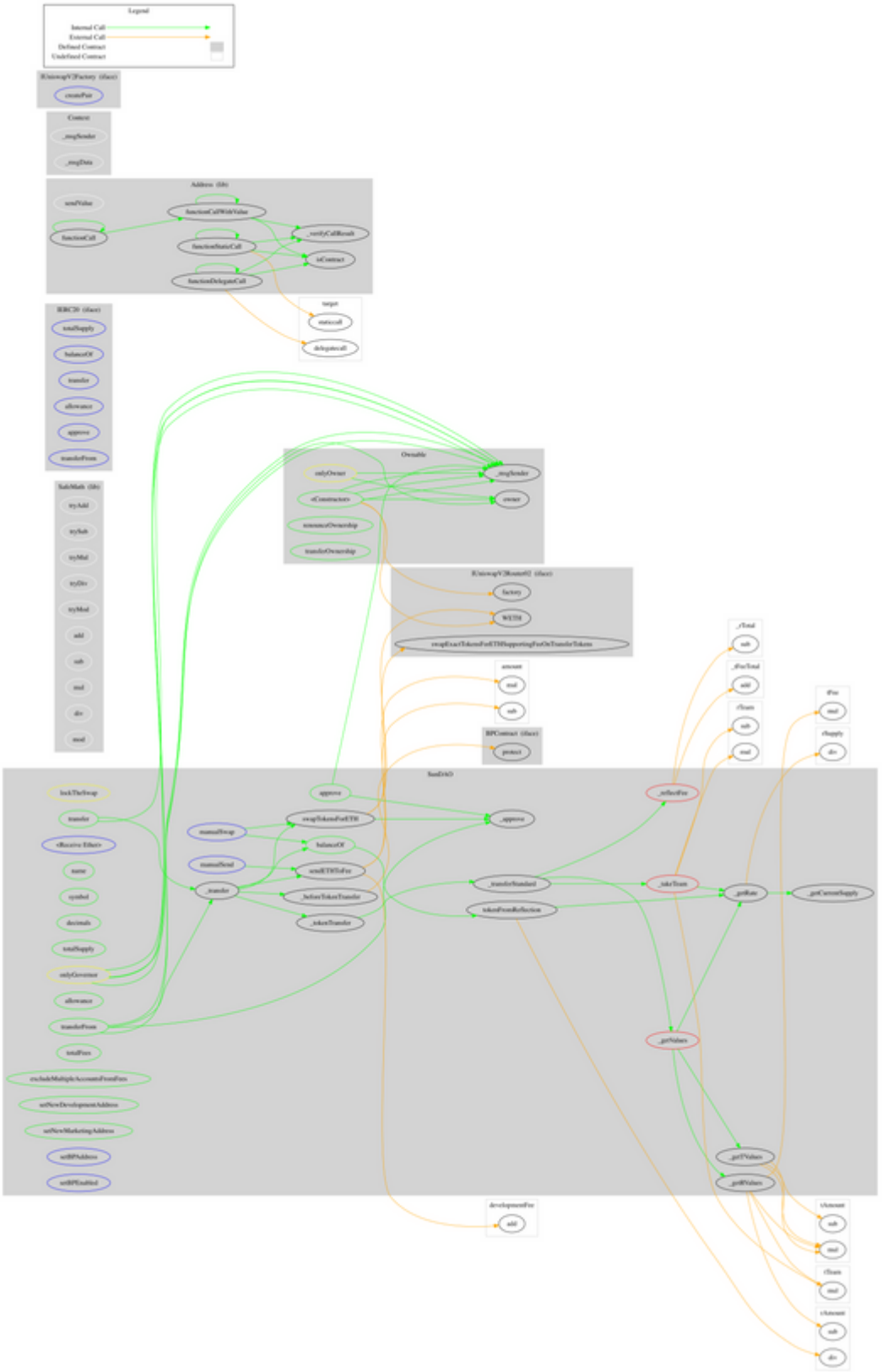
Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Ownable	Implementation	Context		
	<Constructor>	Internal	✓	
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
SafeMath	Library			
	tryAdd	Internal		
	trySub	Internal		
	tryMul	Internal		
	tryDiv	Internal		
	tryMod	Internal		
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
	sub	Internal		
	div	Internal		
	mod	Internal		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-

Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	_verifyCallResult	Private		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
IUniswapV2Factory	Interface			
	createPair	External	✓	-
IUniswapV2Router02	Interface			
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
	factory	External		-
	WETH	External		-
BPContract	Interface			
	protect	External	✓	-
SunDAO	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	<Receive Ether>	External	Payable	-
	name	Public		-

	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	totalFees	Public		-
	tokenFromReflection	Public		-
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_reflectFee	Private	✓	
	_takeTeam	Private	✓	
	_getCurrentSupply	Private		
	_approve	Private	✓	
	_transfer	Private	✓	
	swapTokensForETH	Private	✓	lockTheSwap
	sendETHToFee	Private	✓	
	_tokenTransfer	Private	✓	
	_transferStandard	Private	✓	
	manualSwap	External	✓	onlyGovernor
	manualSend	External	✓	onlyGovernor
	excludeMultipleAccountsFromFees	Public	✓	onlyGovernor
	setNewDevelopmentAddress	Public	✓	onlyGovernor
	setNewMarketingAddress	Public	✓	onlyGovernor
	setBPAddress	External	✓	onlyGovernor
	setBPEnabled	External	✓	onlyGovernor
	_beforeTokenTransfer	Internal	✓	

Contract Flow



Domain Info

Domain Name	sundao.finance
Registry Domain ID	a86396c0f6644988a0089b1ffe81eee7-DONUTS
Creation Date	2022-08-01T03:16:12Z
Updated Date	2022-08-06T03:16:32Z
Registry Expiry Date	2023-08-01T03:16:12Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain has been created in 12 months before the creation of the audit.

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

Summary

The Smart Contract analysis reported one minor severity issue. The contract owner has the authority to transfer funds to the team's wallet. There is also an untrusted source that interacts with the smart contract before each transfer. 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.

Cyberscope 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 Cyberscope 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 Cyberscope 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 Cyberscope team disclaims any liability for the resulting losses.

About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

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.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io