Cyberscope

Audit Report

PokemonFi

June 2022

Type	BEP20
Network	BSC
Address	0x2753dce37a7edb052a77832039bcc9aa49ad8b25
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	SpriteCore
Compiler Version	v0.8.9+commit.e5eed63a
Optimization	200 runs
Licence	None
Explorer	https://bscscan.com/token/0x2753dce37a7edb052a77832039bcc9aa49ad8b25
Symbol	PMF
Decimals	18
Total Supply	1,000,000,000
Domain	pokemonfi.com

Source Files

Filename	**SHA256**
contract.sol	d3e8188fd9db09582a331b0c25c59859ed48976840a6a33b8fd038683aa0ce1d

Audit Updates

Initial Audit	11th June 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

OTUT - Owner Transfer User's Tokens

Criticality	critical
Location	contract.sol#L1796

Description

The contract owner has the authority to transfer any balance to the owner's contract. The owner may take advantage of it by:

- Set the account to an addresses that holds tokens, (`setAccount()`)
- Set the controller role to the owner's address, (`setController()`)
- Execute the `withDraw()` method

```
function withDraw(address to, uint256 amount)
    external
    override
    onlyRole(CONTROL_ROLE)
{
    _transfer(_account, to, amount);
}
```

Recommendation

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.

We state that **the owner privileges are necessary and required for proper protocol operations.** Thus, we emphasise the contract owner to be extra careful with the credentials.

Contract Diagnostics

● Critical ● Medium ● Minor

Severity	Code	Description
●	L01	Public Function could be Declared External
●	L09	Dead Code Elimination
●	L12	Using Variables before Declaration

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L179,187,211,218,230,253,275,298,318,732,747,799,1149,1167,1631,1635,1774,1778,1792

Description

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

```
setAccount
unpause
pause
setTokensOwner
getTokensOwner
renounceRole
revokeRole
renounceOwnership
burnFrom
...
```

Recommendation

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

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L1200,581,591,610,624,670,680,643,653,556,697,1639,1739,1747,1331,1410,1438,1489,1522,1535,941,916,1687,1667,1695,1671,1679

Description

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

```
uint256ToString
uint160ToAddress
bytesToString
addressToUint160
addressToString
toString
toHexString
toTypedDataHash
toEthSignedMessageHash
...
```

Recommendation

Remove unused functions.

L12 - Using Variables before Declaration

Criticality	minor
Location	contract.sol#L1370

Description

The contract is using a variable before the declaration. This is usually happening either if it has not been declared yet or the variable has been declared in a different scope.

```
r
```

Recommendation

The variables should be declared before any usage of them.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
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	✓	
	_spendAllowance	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	verifyCallResult	Internal		
ERC20Burnable	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	

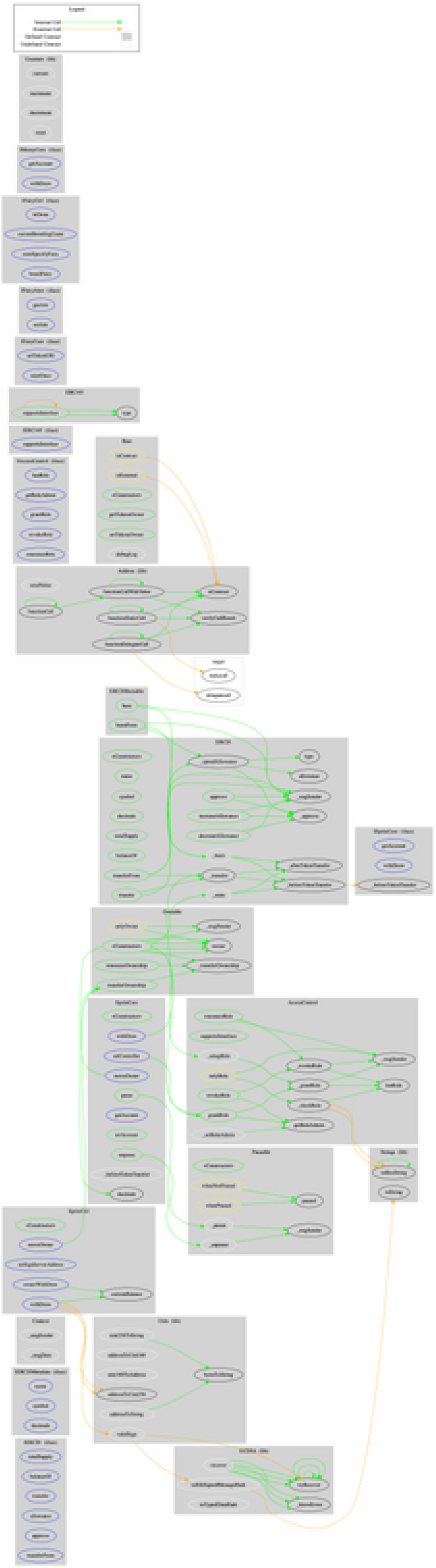
IAccessControl	Interface			
	hasRole	External		-
	getRoleAdmin	External		-
	grantRole	External	✓	-
	revokeRole	External	✓	-
	renounceRole	External	✓	-
Strings	Library			
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
IERC165	Interface			
	supportsInterface	External		-
ERC165	Implementation	IERC165		
	supportsInterface	Public		-
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	Internal	✓	
	_revokeRole	Internal	✓	
Pausable	Implementation	Context		

	<Constructor>	Public	✓	-
	paused	Public		-
	_pause	Internal	✓	whenNotPaused
	_unpause	Internal	✓	whenPaused
ECDSA	Library			
	_throwError	Private		
	tryRecover	Internal		
	recover	Internal		
	tryRecover	Internal		
	recover	Internal		
	tryRecover	Internal		
	recover	Internal		
	toEthSignedMessageHash	Internal		
	toEthSignedMessageHash	Internal		
	toTypedDataHash	Internal		
IFairyCore	Interface			
	setTokenURI	External	✓	-
	mintOnce	External	✓	-
IFairyAttrs	Interface			
	getAttr	External		-
	setAttr	External	✓	-
IFairyCtrl	Interface			
	isOwns	External		-
	currentBreedingCount	External		-
	mintSpecifyFairy	External	✓	-
	breedFairy	External	✓	-
ISpriteCore	Interface			
	getAccount	External		-
	withDraw	External	✓	-

IMoneyCore	Interface			
	getAccount	External		-
	withDraw	External	✓	-
Base	Implementation	Ownable, AccessControl, Pausable		
	<Constructor>	Public	✓	-
	getTokensOwner	Public		-
	setTokensOwner	Public	✓	onlyRole
	debugLog	Internal	✓	
Utils	Library			
	validSign	Internal		
	addressToUint160	Internal		
	uint160ToAddress	Internal		
	addressToUint256	Internal		
	uint256ToString	Internal		
	addressToString	Internal		
	bytesToString	Internal		
Counters	Library			
	current	Internal		
	increment	Internal	✓	
	decrement	Internal	✓	
	reset	Internal	✓	
SpriteCore	Implementation	Base, ERC20, ERC20Burnable, ISpriteCore		
	<Constructor>	Public	✓	ERC20
	setController	External	✓	onlyOwner isContract
	moveOwner	External	✓	onlyOwner isExternal

	pause	Public	✓	onlyOwner whenNotPaused
	unpause	Public	✓	onlyOwner whenPaused
	getAccount	External		onlyRole
	setAccount	Public	✓	onlyOwner isExternal
	withDraw	External	✓	onlyRole
	_beforeTokenTransfer	Internal	✓	whenNotPaused
SpriteCtrl	Implementation	Base		
	<Constructor>	Public	✓	isContract
	moveOwner	External	✓	onlyOwner isExternal
	setSignServerAddress	External	✓	onlyOwner isExternal
	ownerWithDraw	External	✓	onlyRole isExternal
	withDraw	External	✓	isExternal
	currentBalance	Public		-

Contract Flow



Domain Info

Domain Name	pokemonfi.com
Registry Domain ID	2677333296_DOMAIN_COM-VRSN
Creation Date	2022-02-24T14:44:46Z
Updated Date	2022-02-24T14:44:47Z
Registry Expiry Date	2023-02-24T14:44:46Z
Registrar WHOIS Server	whois.maff.com
Registrar URL	http://www.maff.com
Registrar	MAFF Inc.
Registrar IANA ID	817

The domain has been created 4 months before the creation of the audit. It will expire in 9 months.

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

Summary

The Smart Contract analysis reported one critical severity issue. The contract owner has the authority to transfer the user's tokens. We state that the owner privileges are necessary and required for proper protocol operations. Thus, we emphasise the contract owner to be extra careful with the credentials.

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