Cyberscope

Audit Report

SquadSwap

February 2024

Network	BSC
Address	0x2d2567dec25c9795117228adc7fd58116d2e310c
Audited by	© cyberscope

Table of Contents

Review

Contract Name	SquadToken
Compiler Version	v0.8.12+commit.f00d7308
Optimization	200 runs
Explorer	https://bscscan.com/address/0x2d2567dec25c9795117228adc7fd58116d2e310c
Address	0x2d2567dec25c9795117228adc7fd58116d2e310c
Network	BSC
Symbol	SQUAD
Decimals	18
Total Supply	1,000,000,000
Repository	https://github.com/Bit5Tech
SquadSwap Commit	0a65867700e63d4be7083c7911f4da06854d0337
SquadToken Commit	f3718817028eb1b862b153b9a36e3307e9271d60
SquadSwap-v3 Commit	4b84122cb1116545be78851ae263dc11a63a499c

Audit Updates

Initial Audit	24 Nov 2023 https://github.com/cyberscope-io/audits/blob/main/squadswap/v1/audit.pdf
Corrected Phase 2	2 Feb 2023

Source Files

Filename	SHA256
/Squad.sol	e055cd4ec165842b536818ba2984626cdd8d42e08cd5d73a984b0faf03220433

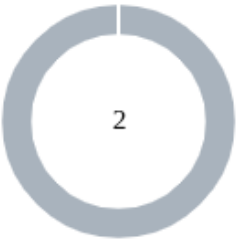
Overview

The `SquadToken` contract, is an implementation of a BEP20 token on the Binance Smart Chain (BSC). This contract adheres to the standards set by the BEP20 protocol, ensuring compatibility and functionality within the BSC ecosystem. The contract is structured to provide a secure and efficient means of creating and managing digital assets, leveraging the robustness of blockchain technology. It includes essential features such as token transfer, balance queries, and allowance management, which are fundamental to the operation of any digital token on a blockchain network.

At the core of the SquadToken contract is the implementation of key functionalities that define its behavior and utility. The contract includes mechanisms for ownership management, allowing the initial deployer of the contract to be designated as the owner. This ownership can be transferred or renounced, providing flexibility and control over the contract's administration. Additionally, the contract incorporates the SafeMath library, a critical component for ensuring safe arithmetic operations, thereby mitigating risks such as overflow and underflow errors. This inclusion is particularly important in the context of financial transactions and token management, where accuracy and security are paramount.

Furthermore, the SquadToken contract is designed with user-centric features that enhance its usability within the BSC network. It supports standard BEP20 functions like transferring tokens between accounts, approving third parties to spend tokens on behalf of the token holder, and querying token balances. These functions are integral to the token's interaction with other contracts and users on the network. The contract's adherence to the BEP20 standard ensures that it can seamlessly integrate with a wide range of decentralized applications (dApps) and services within the Binance Smart Chain ecosystem, making it a versatile and valuable asset for various blockchain-based applications.

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	2

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	2	0	0	0

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	L16	Validate Variable Setters	Unresolved
●	L19	Stable Compiler Version	Unresolved

L16 - Validate Variable Setters

Criticality	Minor / Informative
Location	v2/factory/SquadswapPair.sol#L67,68 v2/factory/SquadswapFactory.sol#L19,45,50
Status	Unresolved

Description

The contract performs operations on variables that have been configured on user-supplied input. These variables are missing of proper check for the case where a value is zero. This can lead to problems when the contract is executed, as certain actions may not be properly handled when the value is zero.

```
token0 = _token0
token1 = _token1
feeToSetter = _feeToSetter
feeTo = _feeTo
```

Recommendation

By adding the proper check, the contract will not allow the variables to be configured with zero value. This will ensure that the contract can handle all possible input values and avoid unexpected behavior or errors. Hence, it can help to prevent the contract from being exploited or operating unexpectedly.

L19 - Stable Compiler Version

Criticality	Minor / Informative
Location	v2/factory/SquadswapPair.sol#L2 v2/factory/SquadswapFactory.sol#L2 v2/factory/SquadswapERC20.sol#L2 v2/factory/libraries/UQ112x112.sol#L2 v2/factory/libraries/Math.sol#L2 v2/factory/interfaces/ISquadswapPair.sol#L2 v2/factory/interfaces/ISquadswapFactory.sol#L2 v2/factory/interfaces/ISquadswapCallee.sol#L2 v2/factory/interfaces/IERC20.sol#L2
Status	Unresolved

Description

The `^` symbol indicates that any version of Solidity that is compatible with the specified version (i.e., any version that is a higher minor or patch version) can be used to compile the contract. The version lock is a mechanism that allows the author to specify a minimum version of the Solidity compiler that must be used to compile the contract code. This is useful because it ensures that the contract will be compiled using a version of the compiler that is known to be compatible with the code.

```
pragma solidity ^0.8.0;
```

Recommendation

The team is advised to lock the pragma to ensure the stability of the codebase. The locked pragma version ensures that the contract will not be deployed with an unexpected version. An unexpected version may produce vulnerabilities and undiscovered bugs. The compiler should be configured to the lowest version that provides all the required functionality for the codebase. As a result, the project will be compiled in a well-tested LTS (Long Term Support) environment.

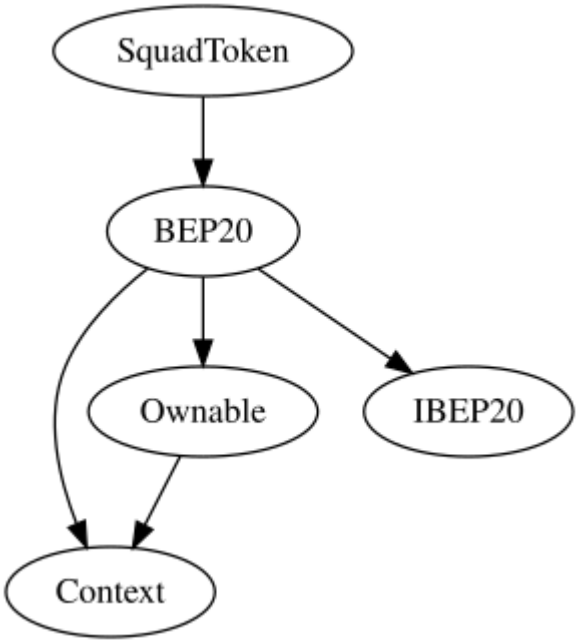
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	_msgSender	Internal		
Ownable	Implementation	Context		
		Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
IBEP20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-

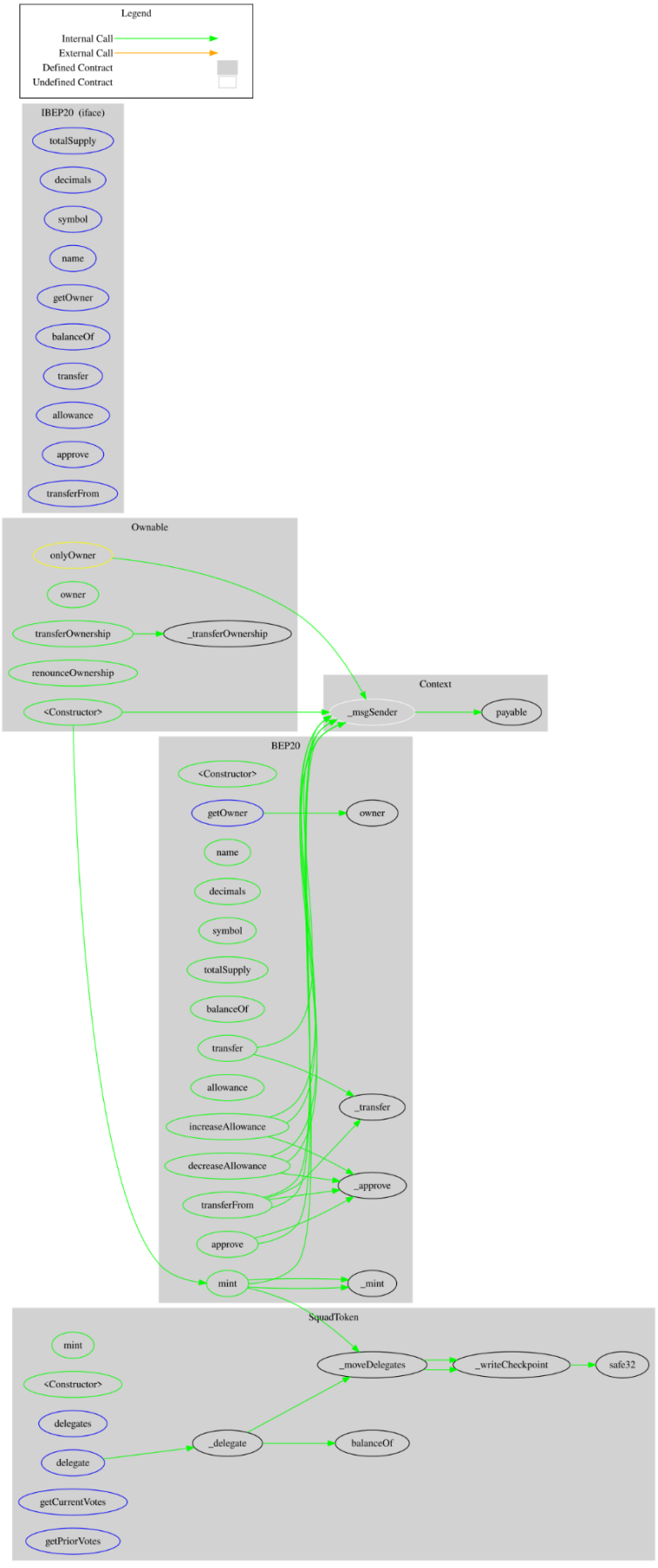
	approve	External	✓	-
	transferFrom	External	✓	-
BEP20	Implementation	Context, IBEP20, Ownable		
		Public	✓	-
	getOwner	External		-
	name	Public		-
	decimals	Public		-
	symbol	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	mint	Public	✓	onlyOwner
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_approve	Internal	✓	
SquadToken	Implementation	BEP20		

	mint	Public	✓	onlyOwner
		Public	✓	-
	delegates	External		-
	delegate	External	✓	-
	getCurrentVotes	External		-
	getPriorVotes	External		-
	_delegate	Internal	✓	
	_moveDelegates	Internal	✓	
	_writeCheckpoint	Internal	✓	
	safe32	Internal		

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
IBEP20 (iface)
totalSupply
decimals
symbol
name
getOwner
balanceOf
transfer
allowance
approve
transferFrom
Ownable
onlyOwner
owner
transferOwnership
_transferOwnership
renounceOwnership
<Constructor>
Context
_msgSender
payable
BEP20
<Constructor>
getOwner
owner
name
decimals
symbol
totalSupply
balanceOf
transfer
allowance
increaseAllowance
decreaseAllowance
transferFrom
approve
mint
_transfer
_approve
_mint
SquadToken
mint
<Constructor>
delegates
delegate
getCurrentVotes
getPriorVotes
_delegate
balanceOf
_moveDelegates
_writeCheckpoint
safe32

Summary

SquadSwap contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io