KISHIELD

Security Audit

MKD Token

May 5, 2022

Table of Contents

1 Audit Summary

2 Project Overview

2.1 Token Summary

2.2 Main Contract Assessed

3 Smart Contract Vulnerability Checks

4 Contract Ownership

4.1 Priviliged Functions

5 Important Notes To The Users

6 Findings Summary

6.1 Classification of Issues

6.1 Findings Table

01 Tax too high (99%)

02 Variables could be declared as constant

03 Public function that could be declared external

04 Missing events arithmetic

05 Division before Multiplication

06 Assigment with no effects

7 Statistics

7.1 Liquidity

7.2 Token Holders

7.3 Liquidity Holders

8 Liquidity Ownership

9 Disclaimer

Audit Summary

This report has been prepared for MKD Token on the Binance Chain network. KISHIELD provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Project Overview

Token Summary

Parameter	Result
Address	0x38e75cd73754134c0bf1846b3a3503fb5c517633
Name	MKD
Token Tracker	MKD (MKD)
Decimals	18
Supply	10,000,000
Platform	Binance Chain
compiler	v0.8.7+commit.e28d00a7
Optimization	Yes with 200 runs
LicenseType	Unlicense
Language	Solidity
Codebase	https://bscscan.com/address/0x38e75cd73754134c0bf1846b3a3503fb5c517633
Url	strikecryptobsc.com

Main Contract Assessed

Name	Contract	Live
MKD	0x38e75cd73754134c0bf1846b3a3503fb5c517633	Yes

Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	✓ Low / No Risk
Code With No Effects	Complete	Complete	✓ Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	✓ Low / No Risk
Hash Collisions With Multiple Variable Length Arguments	Complete	Complete	✓ Low / No Risk
Unexpected Ether balance	Complete	Complete	✓ Low / No Risk
Presence of unused variables	Complete	Complete	✓ Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	✓ Low / No Risk
Typographical Error	Complete	Complete	✓ Low / No Risk
DoS With Block Gas Limit	Complete	Complete	✓ Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	✓ Low / No Risk
Insufficient Gas Griefing	Complete	Complete	✓ Low / No Risk
Incorrect Inheritance Order	Complete	Complete	✓ Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	✓ Low / No Risk
Requirement Violation	Complete	Complete	✓ Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	✓ Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	✓ Low / No Risk

Vulnerability	Automatic Scan	Manual Scan	Result
Authorization through tx.origin	Complete	Complete	✓ Low / No Risk
Delegatecall to Untrusted Callee	Complete	Complete	✓ Low / No Risk
Use of Deprecated Solidity Functions	Complete	Complete	✓ Low / No Risk
Assert Violation	Complete	Complete	✓ Low / No Risk
Reentrancy	Complete	Complete	✓ Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	Complete	✓ Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	✓ Low / No Risk
Unchecked Call Return Value	Complete	Complete	✓ Low / No Risk
Outdated Compiler Version	Complete	Complete	✓ Low / No Risk
Integer Overflow and Underflow	Complete	Complete	✓ Low / No Risk
Function Default Visibility	Complete	Complete	✓ Low / No Risk

Contract Ownership

The contract ownership of MKD is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0xF3180e84f9932c32504dBD419CadE4DeE202E590 which can be viewed from:
HERE

The owner wallet has the power to call the functions displayed on the priviliged functions chart below, if the owner wallet is compromised this privileges could be exploited.

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

Important Notes To The Users:

- The owner cannot mint tokens after intial deployment.
- The owner cannot stop Trading.
- The owner cannot set the fees over 20% for both buy and sell.
- There is a 99% tax fee for the 3 blocks after the token launch.
- There is a sell cooldown of 60 seconds between sells.
- Once the owner renounces ownership of the contract, none of the following are applicable.
- [WARNING] The owner can change the 99% tax block deadline before launch with no restrictions. If the owner changes it to a high value there will be 99% tax forever.
- The owner can change the max buy/sell amount as long as the amount is bigger than 10,000 Tokens.
- The owner can change the max wallet amount as long as the amount is bigger than 10,000 Tokens.
- The owner can enable/disable the liquidity addition mechanism but this stops the team from getting the fee revenue.
- The owner can change the coolDownTime and enable/disable the cooldown mechanism as long as the coolDownTime is less than 5 minutes.
- The owner can add/remove addresses from fees.
- The owner can transfer BNB and tokens out of the contract.
- No high-risk Exploits/Vulnerabilities Were Found in token Source Code other than changes in the deadline.

Technical Findings Summary

Classification of Issues

Severity	Description
🔴 High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency
🟠 Medium	Bugs or issues with that may be subject to exploit, though their impact is somewhat limited.Issues under this classification are recommended to be fixed as soon as possible.
🟡 Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
🟣 Info	Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

Findings

Severity	Found
🔴 High	1
🟠 Medium	0
🟡 Low	0
🟣 Info	5
Total	6

Findings

Tax too high (99%)

ID	Severity	Contract	Function
01	🔴 High	MKD	Function updatedeadline() & _transfer()

Description

The owner can change the 99% tax block deadline before launch with no restrictions. If the owner changes it to a high value there will be 99% tax forever for non-tax-exempt users.

Recommendation

We recommend adding a require statement to limit the length of the deadline or delete the updatedeadline function.

Variables could be declared as constant

ID	Severity	Contract	Function
02	🟣 Informational	MKD	variable launchtax

Description

Gas Optimization. Variables that are never changed could be declared as constant.

Recommendation

We recommend declaring those variables as constant.

Public function that could be declared external

ID	Severity	Contract	Function
03	● Informational	MKD	Functions renounceOwnership, transferOwnership

Description

Gas Optimization. Public function that could be declared external

Recommendation

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

Missing events arithmetic

ID	Severity	Contract	Function
04	● Informational	MKD	Missing events for EnableTrading, updatedeadline, updateCooldown, updateMaxBuyTxLimit, updateMaxSellTxLimit, updateMaxWalletlimit

Description

Functions that change critical arithmetic parameters should emit an event.

Recommendation

Emit corresponding events for critical parameter changes.

Division before Multiplication

ID	Severity	Contract	Function
05	● Informational	MKD	function handle_fees()

Description

Precision Loss. 'unitBalance = deltaBalance / (denominator - swapTaxes.liquidity) => bnbToAddLiquidityWith = unitBalance * swapTaxes.liquidity'. Division before multiplication can result in truncation and less accurate results

Recommendation

Multiplication should be performed before division to not lose precision.

Assigment with no effects

ID	Severity	Contract	Function
06	● Informational	MKD	Variables _liquidityMutex, providingLiquidity, tradingEnabled == false

Description

Bools variables in solidity are set to false by default.

Recommendation

We recommend deleting the initilization of the boolean variable to false

Priviliged Functions (onlyOwner)

Function Name	Parameters	Visibility
renounceOwnership	none	public
transferOwnership	address newOwner	public
updateLiquidityProvide	bool state	external
updateLiquidityTreshhold	uint256 new_amount	external
SetBuyTaxes	uint256 _marketing, uint256 _liquidity, uint256 _gamedev, uint256 _dev	external
SetSellTaxes	uint256 _marketing, uint256 _liquidity, uint256 _gamedev, uint256 _dev	external
updateRouterAndPair	address newRouter, address newPair	external
EnableTrading	none	external
updatedeadline	uint256 _deadline	external
updateMarketingWallet	address newWallet	external
updateGamedevWallet	address newWallet	external
updateDevWallet	address newWallet	external
updateCooldown	bool state, uint256 time	external
updateAllowedTransfer	address account, bool state	external
bulkAllowedTransfer	calldata accounts, bool state	external

Function Name	Parameters	Visibility
updateExemptFee	address _address, bool state	external
bulkExemptFee	calldata accounts, bool state	external
updateMaxBuyTxLimit	uint256 maxBuy	external
updateMaxSellTxLimit	uint256 maxSell	external
updateMaxWalletlimit	uint256 amount	external
rescueBNB	uint256 weiAmount	external
rescueBSC20	address tokenAdd, uint256 amount	external

Statistics

Liquidity Info

Parameter	Result
Pair Address	0xAbC01c04166F0575e80f885c2B4c27a68e411F85
MKD Reserves	0.00 MKD
BNB Reserves	0.00 BNB
Liquidity Value	$0 USD

Token (MKD) Holders Info

Parameter	Result
MKD Percentage Burnt	0.00%
MKD Amount Burnt	0 MKD
Top 10 Percentage Own	100.00%
Top 10 Amount Owned	10,000,000 MKD
Top 10 Aprox Value	$NaN USD

LP (MKD/BNB) Holders Info

Parameter	Result
MKD/BNB % Burnt	0.00%
MKD/BNB Amount Burnt	0 MKD
Top 10 Percentage Owned	0.00%
Top 10 Amount Owned	0 MKD
Locked Tokens Percentage	0.00%
Locked Tokens Amount	0 MKD

* All the data diplayed above was taken on-chain at block 17543469
* The tokens on industry-standard burn wallets are not included on the top 10 wallets calculations

Liquidity Ownership

The token does not have liquidity at the moment of the audit, block 17543469

KISHIELD

Disclaimer

KISHIELD has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and KISHIELD is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will KISHIELD or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by KISHIELD is subject to dependencies and 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.