KISHIELD

Security Audit

mainfarm.io MasterChef

September 14, 2022

Audit Passed

Table of Contents

Audit Passed

✓

Audit Summary

This report has been prepared for mainfarm.io MasterChef on the BSC 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.

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	0xDd0B606C24327CF116f6E8f38bE0A1a81aAd3120
Name	mainfarm.io MasterChef
Platform	BSC
compiler	v0.6.12+commit.27d51765
Optimization	Yes with 1 runs
LicenseType	None
Language	Solidity
Codebase	https://bscscan.com/address/0xDd0B606C24327CF116f6E8f38bE0A1a81aAd3120#code
Url	https://mainfarm.io

Main Contract Assessed

Name	Contract	Live
mainfarm.io MasterChef	0xDd0B606C24327CF116f6E8f38bE0A1a81aAd3120	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 mainfarm.io MasterChef 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 0xb00f980f9c107b650bf0ba5d87c158f3e6141e2f 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.

Findings Summary

Classification of Issues

All Issues Are Informational.

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	0
🟠 Medium	0
🟡 Low	0
🟣 Info	4
Total	4

Findings

Unused Functions

ID	Severity	Contract	Location
01	● Informational	mainfarm.io MasterChef	Functions Address.functionCall, Address.functionCallWithValue, Address.functionCallWithValue, Address.sendValue , BEP20._burnFrom , Context._msgData() , SafeBEP20.safeDecreaseAllowance , SafeBEP20.safeIncreaseAllowance , SafeMath.min, SafeMath.mod, SafeMath.mod, SafeMath.sqrt

Finding Description

Functions are not used by the contract

KISHIELD Recommendation

Remove the unused functions

Missing events arithmetic

ID	Severity	Contract	Location
02	● Informational	mainfarm.io MasterChef	Functions MasterChef.updateMultiplier, MasterChef.add, MasterChef.set

Finding Description

Functions that change critical arithmetic parameters should emit an event.

KISHIELD Recommendation

Make the function emit an event.

Public function that could be declared external

ID	Severity	Contract	Location
03	● Informational	mainfarm.io MasterChef	Functions updateMultiplier, add, set, setMigrator, migrate, deposit, withdraw, enterStaking, leaveStaking, emergencyWithdraw, dev

Finding Description

Gas Optimization. Public function that could be declared external

KISHIELD Recommendation

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

Comment Typo

ID	Severity	Contract	Location
04	● Informational	mainfarm.io MasterChef	Line 1528

Finding Description

The linked comment statement contains a typo in its text, the word 'poitns'.

KISHIELD Recommendation

We advise that the comment text is corrected

Priviliged Functions (onlyOwner)

Function Name	Parameters	Visibility
Ownable.renounceOwnership	none	public
Ownable.transferOwnership	address newOwner	public
CakeToken.mint	address _to, uint256 _amount	public
SyrupBar.mint	address _to, uint256 _amount	public
SyrupBar.burn	address _from, uint256 _amount	public
SyrupBar.safeCakeTransfer	address _to, uint256 _amount	public
MasterChef.updateMultiplier	uint256 multiplierNumber	public
MasterChef.add	uint256 _allocPoint, calldata _lpToken, bool _withUpdate	public
MasterChef.set	uint256 _pid, uint256 _allocPoint, bool _withUpdate	public
MasterChef.setMigrator	calldata _migrator	public

Important Notes To The Users:

- This MasterChef contract is a fork of PancakeSwap MasterChef V1 at 0x73feaa1eE314F8c655E354234017bE2193C9E24E
- The MasterChef contract allows users to stake tokens in order to earn rewards in the form of a designated reward token.
- The owner can add new staking pools at any time.
- The owner can change all pools' allocation points at any time.
- No high-risk Exploits/Vulnerabilities were found in token source code.

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.