Smart Contract Audit Report

Ethereum

Littlemami

V0.1

NO.202304040001

April 4th, 2023

Contents

1 Report Overview

Binenet security team have audited the Littlemami, 2 risks was identified in Littlemami. users should pay attention to the following aspects when interacting with this project.

Contract Code	Function	Security Level	Status
LMC.sol	mint	Info	---
MamiProtocol.sol	sync	Info	---

***Risk Description: The owner can mint LMC token and a risk of conditional competition with sync function.**

2 Asset Management Security Assessment

Asset Type	Function	Security Level
User Mortgage Token Assets	mint, burn, burnFrom	Info
Users Mortgage Platform Currency Assets	mint, burn, burnFrom	Info

Description: Check the **management security of digital currency assets** transferred by users in the contract business logic. Observe whether there are security risks that may cause the loss of customer funds, such as the **digital currency assets** transferred into the contract are **incorrectly recorded or transferred out by mistake**.

3 Audit Overview

3.1 Project Information

Mami Protocol is an open-source protocol that facilitates efficient and secure liquidity for NFT trading pairs. It enables the creation of ERC20 and ERC721 trading pairs and allows users to earn liquidity tokens by staking ERC20 and ERC721 tokens.

The Mami Protocol is designed to solve the liquidity problem in the NFT market. By allowing users to create trading pairs and earn liquidity tokens, it provides an efficient and secure way to trade NFTs. It also enables users to increase or destroy liquidity and swap ERC20 and ERC721 tokens with a fee.

The Mami Protocol is part of the decentralized finance (DeFi) ecosystem, which is rapidly growing and evolving. As more NFTs are created and traded, the demand for efficient and secure liquidity solutions will increase. The Mami Protocol is well-positioned to meet this demand and continue to play a significant role in the DeFi space.

3.2 Audit Information

Project Name	Littlemami
Platform	Ethereum
Audit Scope	LMC.sol#be6c2e2478fced2c30c24f206e35a5d4#https://etherscan.io/address/0x8983cf891867942d06ad6ceb9b9002de860e202d MamiProtocol.sol#2b8a54838e57810d17048782730f3283 MamiStakeManager.sol#71e08fe896cefc658eb9a07a1d396296

3.3 External Visibility Analysis

Function	Visibility	State Change	Modifier	Payable	Description
mint	external	True	onlyRole	---	LMC

burn	public	True	---	---	LMC
burnFrom	public	True	---	---	LMC
stake	external	True	---	---	MamiErc20StakePool
unStake	external	True	---	---	MamiErc20StakePool
stake	external	True	---	---	MamiErc721StakePool
unStake	external	True	---	---	MamiErc721StakePool
addLiquidity	external	True	---	---	MamiRouter
addLiquidityETH	external	True	---	payable	MamiRouter
removeLiquidity	public	True	---	---	MamiRouter
removeLiquidityETH	external	True	---	---	MamiRouter
swapERC20ForExactERC721	external	True	---	---	MamiRouter
swapExactERC721ForERC20	external	True	---	---	MamiRouter
swapETHForExactERC721	external	True	---	payable	MamiRouter
swapExactERC721ForETH	external	True	---	---	MamiRouter

3.4 Audit Process

Audit time: 2023.4.1 - 2023.4.4

Audit methods: Static Analysis, Dynamic Testing, Typical Case Testing and Manual Review.

Audit team: Binenet Security Team.

4 Security Finding Details

4.1 Token mint function

Severity Level : Info

Lines : LMC.sol # L16-26

Description: There is a mint function in the contract, which is controlled by the owner.

```
ftrace | funcSig
16      function mint(
17          address _account,
18          uint256 _amount
19      ) external onlyRole(MINT_ROLE) {
20          require(
21              _amount + totalSupply() <= MAX_SUPPLY,
22              "LM : Out of max supply"
23          );
24          _mint(_account, _amount);
25      }
26  }
```

Recommendations: Special attention.

Status : Fixed.

4.2 Release rate changeable

Severity Level : Info

Lines : MamiStakeManager.sol # L367-372

Description: The owner can modify the mining release rate.

```
ftrace | funcSig
367     function changeRate(
368         address _pool,
369         uint256 _rewardsPerBlock
370     ) public onlyOwner {
371         IMamiStakePool(_pool).changeRate(_rewardsPerBlock);
372     }
```

Recommendations: Special attention.

Status : Fixed.

4.3 Conditional competition with sync function

Severity Level : Info

Lines : MamiProtocol.sol # L289-293

Description: There is a risk of conditional competition with sync function

```
ftrace | funcSig
289     function sync() external {
290         (uint256 erc721Amount, uint256 erc20Amount) = getPairRemainAmount();
291         _sync(erc721Amount, erc20Amount);
292     }
293
```

Recommendations: Add nonReentrant modifier.

Status : Fixed.

5 Audit Categories

Categories	Subitems
Business Security	Transfer token function
	Mint token and burn token vulnerability
	Contract logic function
	Mining pool deposit and withdrawal function
	Reasonableness of agreement amendment
	Functional design
	Dos caused by time
	Insecure oracles and their design
	Deployer private key leak hazard
General Vulnerability	Compiler version security
	Redundant code
	Use of safemath library
	Not recommended encoding
	Use require/assert mistakely
	Fallback function safety
	tx.origin authentication
	Owner permission control
	Gas consumption detection
	Call injection attack
	Low-level function safety
	Additional token vulnerabilities
	Access control
	Numeric overflow detection
	Arithmetic precision error
	Misuse of random number detection
	Unsafe external call
	Variable override
	Uninitialized storage pointer

	Return value call validation
	Transaction order dependent detection
	Timestamp dependent attack
	Denial of service attack detection
	Fake recharge vulnerability detection
	Reentrancy Attack Detection
	Replay attack detection
	Reordering attack detection

6 Explanation Of Vulnerability Rating

Vulnerability Rating	Rating Description
High Risk Vulnerabilities	Vulnerabilities that can directly cause the loss of token contracts or user funds, such as: overflow、reentrancy 、false recharge， which can cause the value of tokens to be zeroed, or causing false exchanges to lose tokens, or causing losing ETH or tokens, etc; Vulnerabilities that can cause loss of ownership of token contracts, such as: access control flaws of key functions, call injection leading to access control bypass of key functions, etc; Vulnerabilities that can cause token contracts to fail to work properly, such as: denial of service vulnerabilities caused by sending ETH to malicious addresses, and denial of service vulnerabilities caused by gas exhaustion;
Medium Risk Vulnerability	High-risk vulnerabilities that require specific addresses to be triggered, such as overflow that can only be triggered by token contract owners; access control flaws of non-critical functions, logic design flaws that cannot cause direct financial losses, etc;
Low Risk Vulnerability	Vulnerabilities that are difficult to be triggered, vulnerabilities that cause limited harm after triggering, such as overflow vulnerabilities that require a large amount of ETH or tokens to be triggered, vulnerabilities that the attacker cannot directly profit after triggering overflow, and transaction sequence-dependent risks triggered by specifying high gas wait;

7 Statement

Binenet only issues this report based on the facts that have occurred or existed before the issue of this report, and assumes corresponding responsibilities for it. For the facts that occurred or existed after the issuance, we cannot judge the security status of the smart contract , and we will not be responsible for it.

This report does not include external contract calls , new types of attacks that may appear in the future, and contract upgrades or tampered codes (with the development of the project side, smart contracts may add new pools, new functional modules, new external contract calls, etc.), does not include front-end security and server security.

The documents and materials provided to us by the information provider as of the date of this report.

Binenet assumes that there is no missing, tampered, deleted or concealed information provided. If the information provided is missing, tampered, deleted, concealed or reflected inconsistent with the actual situation, Binenet shall not be liable for any losses and adverse effects resulting therefrom.

8 About Binenet

Founded in June 2021, Binenet is a dedicated and pure blockchain security company, focusing on accurate, efficient and intelligent blockchain threat detection and response. Committed to providing users with professional products and dedicated services in the field of blockchain security. Business functions cover penetration testing, code auditing, emergency response, on-chain data monitoring, AML anti-money laundering, etc., covering all aspects of blockchain ecosystem security.

Official Website
https://binenet.com

Telegram
https://t.me/binenetxyz

Twitter
https://twitter.com/binenetxyz

E-mail
team@binenet.com