REDMULLET
TECH

Smart Contract Audit Report

IPMB Token

Nov 30th, 2023

Table of Contents

Executive Summary

In November 2023, Red Mullet Tech Ltd conducted a security audit of the IPMB Token (IPMB) smart contract. Our goal was to thoroughly assess potential vulnerabilities to ensure the security of user funds. This report summarizes our findings and recommendations. The examination has been performed using white-box testing method and manual review techniques utilizing tailor made unit tests on the smart contract’s source code.

Audit Process

Our audit rigorously tested the IPMB smart contracts against both standard and unconventional attack vectors. Key aspects of our methodology included:

- Comprehensive testing against known and emerging attack vectors.
- In-depth codebase analysis for adherence to current best practices and industry standards.
- Verification that the contract logic aligns with the client's specifications and intentions.
- Comparison of contract structure and implementation with those of leading industry standards.
- Detailed manual review of the entire codebase by experienced industry professionals.

Overview

Project Summary

Project Name	IPMB Token (ERC20)
Platform	Polygon (EVM)
Language	Solidity
Contract Address	0xFF22c94FFb6bB5d1DF18bEb5fd1dFE7583D3B214 (18 DECIMALS)
Codebase	https://github.com/IpmbOfficial/IPMB

Audit Summary

Delivery Date	Nov 30, 2023
Audit Methodology	Whitebox Testing, Manual Review

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged
● High-severity	0	0	0	0
● Medium-severity	0	0	0	0
● Low-severity	2	0	0	2

Audit Scope

ID	File	SHA256 Checksum
IPMB	IPMB.sol	e79216d40b1f9fa506986f0f5df23fef9d22dfe8acc0b94f199f577f576f66ff

Findings

Our audit reported a total of 2 findings, categorized as follows:

🟥	High-severity issue(s)	0 (0%)
🟧	Medium-severity issue(s)	0 (0%)
🟦	Low-severity issue(s)	2 (100%)

Low-severity issue(s)

1. **Owner Privileges**

The contract grants the owner the ability to transfer or renounce ownership, which poses potential risks if misused.

2. **Missing Checks on Array Lengths in batchTransfers()**

Discrepancies in array lengths can lead to processing errors or out-of-bound issues, potentially affecting transaction integrity.

No high or medium-severity issues were found, and no critical security risks were identified.

Recommendations

Based on our findings, we recommend the following:

- Implement safeguards or restrictions on the transfer of ownership rights.
- Introduce validation checks to ensure the uniformity of array lengths in the batchTransfers() function.

IPMB Token Test-bench Results

Verify Fixture

√ Contracts are deployed

Check Info

√ #name
√ #symbol
√ #decimals

Check Deployer balance

√ #balanceOf

Transfer 50 tokens

√ #transfer
√ #balanceOf (sender)
√ #balanceOf (recipient)

Burn 100 tokens

√ #burn
√ #balanceOf

Approve spender

√ #approve
√ #allowance

Increase & decrease allowance spender

√ #increaseAllowance
√ #allowance (after increase)
√ #decreaseAllowance
√ #allowance (after decrease)

Transfer on behalf of owner

√ #transferFrom
√ #allowance (after transfer)
√ #balanceOf

Burn on behalf of owner

√ #burnFrom
√ #allowance (after burn)
√ #balanceOf

Batch transfer of 100 tokens

√ #batchTransfers
√ #balanceOf (sender)
√ #balanceOf (first recipient)
√ #balanceOf (second recipient)

Transfer Ownership

- √ #transferOwnership
- √ #owner
- √ #balanceOf (new owner)

Contract Performance Metrics

Solc version: 0.8.19	Optimizer enabled: true	Runs: 200	Block limit: 30000000 gas

Methods

Contract	Method	Min	Max	Avg	# calls	usd (avg)
IPMBToken	approve	-	-	46283	1	-
IPMBToken	batchTransfers	-	-	61715	1	-
IPMBToken	burn	-	-	33713	1	-
IPMBToken	burnFrom	-	-	41569	1	-
IPMBToken	decreaseAllowance	-	-	29426	1	-
IPMBToken	increaseAllowance	-	-	29464	1	-
IPMBToken	transfer	-	-	51460	1	-
IPMBToken	transferFrom	-	-	59357	1	-
IPMBToken	transferOwnership	-	-	28678	1	-

Deployments

Deployment	Min	Max	Avg	% of limit
IPMBToken	-	-	965577	3.2%

Disclaimer

This report is subject to the terms and conditions set forth in the Services Agreement, including without limitation, descriptions of services, confidentiality, disclaimer, and limitation of liability, provided to you ("Customer" or the "Company") in connection with the Agreement. This report, provided in connection with the Services outlined in the Agreement, is for the Company's use only, as permitted under the Agreement's terms and conditions. It may not be transmitted, disclosed, referred to, or relied upon by any person for any purposes, nor may copies be provided to anyone other than the Company without Red Mullet Tech's prior written consent in each instance.

This report is not an endorsement or disapproval of any project or team. It should not be considered as an indication of the economics or value of any product or asset created by a team or project that contracts Red Mullet Tech for a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed and should not be used for investment decisions or as investment advice.

Blockchain technology and cryptographic assets carry ongoing risks. Red Mullet Tech aims to reduce attack vectors and variance associated with new and changing technologies but does not claim any guarantee of security or functionality. Our assessment services depend on continuous development and are provided on an as-is, where-is, and as-available basis.

ALL SERVICES, ASSESSMENT REPORTS, WORK PRODUCTS, AND OTHER MATERIALS, OR ANY RESULTS OF THEIR USE ARE PROVIDED “AS IS” AND “AS AVAILABLE,” WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, RED MULLET TECH DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. RED MULLET TECH MAKES NO WARRANTY THAT THE SERVICES, ASSESSMENT REPORTS, OR MATERIALS WILL MEET CUSTOMER’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE.

NEITHER RED MULLET TECH NOR ANY OF ITS AGENTS MAKES ANY REPRESENTATION OR WARRANTY AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. RED MULLET TECH ASSUMES NO LIABILITY OR RESPONSIBILITY FOR ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS, OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THEIR USE.

THE SERVICES AND ASSESSMENT REPORTS ARE SOLELY PROVIDED TO THE CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO ANY OTHER PERSON WITHOUT RED MULLET TECH’S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

About

Red Mullet Tech Ltd is founded by leading Academics that specialize in building secure, trusted, and decentralized software solutions leveraging Web3 Technology. Our vast experience enables our clients to stay at the forefront of technological advancements and optimize their existing processes.

For more information, visit www.redmullet.com