

SALUS SECURITY

FEB 2025



# CODE SECURITY ASSESSMENT

MEMEMARKET

# Overview

## Project Summary

- Name: MemeMarket - \$MFUN
- Platform: Solana
- Address: [6CfnWgNKqJWWTTZsU2GswHNNKyXR4VfjygUZ73kh3U1L](#)
- Audit Range: See [Appendix - 1](#)

## Project Dashboard

### Application Summary

Name	MemeMarket - \$MFUN
Version	v2
Type	Solidity
Dates	Feb 20 2025
Logs	Feb 10 2025; Feb 20 2025

### Vulnerability Summary

Total High-Severity issues	0
Total Medium-Severity issues	0
Total Low-Severity issues	1
Total informational issues	0
Total	1

## Contact

E-mail: [support@salusec.io](mailto:support@salusec.io)

## Risk Level Description

<b>High Risk</b>	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for clients' reputations or serious financial implications for clients and users.
<b>Medium Risk</b>	The issue puts a subset of users' sensitive information at risk, would be detrimental to the client's reputation if exploited, or is reasonably likely to lead to a moderate financial impact.
<b>Low Risk</b>	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.
<b>Informational</b>	The issue does not pose an immediate risk, but is relevant to security best practices or defense in depth.

# Content

<b>Introduction</b>	<b>4</b>
1.1 About SALUS	4
1.2 Audit Breakdown	4
1.3 Disclaimer	4
<b>Findings</b>	<b>5</b>
2.1 Summary of Findings	5
2.2 Notable Findings	6
1. Centralization risk	6
2.3 Informational Findings	7
<b>Appendix</b>	<b>8</b>
Appendix 1 - Files in Scope	8

# Introduction

## 1.1 About SALUS

At Salus Security, we are in the business of trust.

We are dedicated to tackling the toughest security challenges facing the industry today. By building foundational trust in technology and infrastructure through security, we help clients to lead their respective industries and unlock their full Web3 potential.

Our team of security experts employ industry-leading proof-of-concept (PoC) methodology for demonstrating smart contract vulnerabilities, coupled with advanced red teaming capabilities and a stereoscopic vulnerability detection service, to deliver comprehensive security assessments that allow clients to stay ahead of the curve.

In addition to smart contract audits and red teaming, our Rapid Detection Service for smart contracts aims to make security accessible to all. This high calibre, yet cost-efficient, security tool has been designed to support a wide range of business needs including investment due diligence, security and code quality assessments, and code optimisation.

We are reachable on Telegram (<https://t.me/salusec>), Twitter ([https://twitter.com/salus\\_sec](https://twitter.com/salus_sec)), or Email ([support@salusec.io](mailto:support@salusec.io)).

## 1.2 Audit Breakdown

The objective was to evaluate the repository for security-related issues, code quality, and adherence to specifications and best practices. Possible issues we looked for included (but are not limited to):

- Risky external calls
- Integer overflow/underflow
- Transaction-ordering dependence
- Timestamp dependence
- Access control
- Call stack limits and mishandled exceptions
- Number rounding errors
- Centralization of power
- Logical oversights and denial of service
- Business logic specification
- Code clones, functionality duplication

## 1.3 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release and does not give any warranties on finding all possible security issues with the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues.

# Findings

## 2.1 Summary of Findings

ID	Title	Severity	Category	Status
1	Centralization risk	Low	Centralization	Mitigate

## 2.2 Notable Findings

Significant flaws that impact system confidentiality, integrity, or availability are listed below.

<b>1. Centralization risk</b>	
Severity: Low	Category: Centralization
Target: <ul style="list-style-type: none"><li>- \$MFUN</li></ul>	

### Description

There is a privileged minter address for \$MFUN. This account then has full control over the token distribution. If it is an EOA account, any compromise of its private key could drastically affect the project. For example, an attacker gaining access to the private key could manipulate the price of \$MFUN on the DEX.

### Recommendation

We recommend transferring privileged accounts to multi-sig accounts with timelock governors for enhanced security. This ensures that no single person has full control over the accounts and that any changes must be authorized by multiple parties.

### Status

The team has already used a multi-sig account to mitigate this issue.

## 2.3 Informational Findings

No informational issues were found.



# Appendix

## Appendix 1 - Files in Scope

This audit covered the token based on Token 2022

[6CfnWgNKqJWWTTZsU2GswHNNKyXR4VfjygUZ73kh3U1L](#).