SALUS SECURITY

MAY 2025

CODE SECURITY ASSESSMENT

CUDIS

Overview

Project Summary

- Name: CUDIS
- Platform: Solana chains
- Language: Rust
- Repository:
    - https://solscan.io/token/CudisfkgWvMKnZ3TWf6iCuHm8pN2ikXhDcWytwz6f6RN
- Audit Range: See Appendix - 1

Project Dashboard

Application Summary

Name	CUDIS
Version	v2
Type	Solana
Dates	May 12 2025
Logs	May 12 2025; May 12 2025

Vulnerability Summary

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

Contact

E-mail: support@salusec.io

Risk Level Description

High Risk	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.
Medium Risk	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.
Low Risk	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.
Informational	The issue does not pose an immediate risk, but is relevant to security best practices or defense in depth.

Content

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), or Email (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	The token metadata can be modified	Informational	Centralization	Resolved

2.2 Informational Findings

1. The token metadata can be modified

Severity: Informational	Category: Centralization
Target: - https://explorer.solana.com/address/CudisfkgWvMKnZ3TWf6iCuHm8pN2ikXhDcWytwz6f6RN	

Description

During deployment, the audited token used the `mql-metadata-token` program to create its token metadata.

The `updateAuthority` can update the token's metadata by invoking the `UpdateMetadataAccountV2` instruction of the `mql-metadata-token program`. This means that fields such as the token's `name`, `symbol`, and `uri` may be modified. Additionally, the `sellerFeeBasisPoints`, which may be retrieved by secondary marketplaces to determine royalties, can also be changed.

The current `updateAuthority` is a user account controlled by a key pair. If the private key is leaked or compromised, the token metadata could be maliciously modified.

token-metadata json on solana explorer

```
{
  key:4
  updateAuthority:"2n5aS2xbcWjFeNSoZD3FSvJueqoj8Wer3Aph4cGwB6fC"
  mint:"CudisfkgWvMKnZ3TWf6iCuHm8pN2ikXhDcWytwz6f6RN"
  data:{
    name:"CUDIS"
    symbol:"CUDIS"
    ...
    sellerFeeBasisPoints:0
  }
  primarySaleHappened:0
  isMutable:1
  ...
}
```

Recommendation

It is recommended to use a multisig account as the `updateAuthority` to mitigate the risk.

Status

This issue has been resolved by the team.

Appendix

Appendix 1 - Files in Scope

This audit covered on-chain token: CudisfkgWvMKnZ3TWf6iCuHm8pN2ikXhDcWytwz6f6R