



Full Audit Report

Cryptsurance Security Assessment



Cryptosurance Security Assessment

FULL AUDIT REPORT

Security Assessment by SCRL on **Monday, January 13, 2025**

SCRL is deliver a security solution for Web3 projects by expert security researchers.



Executive Summary

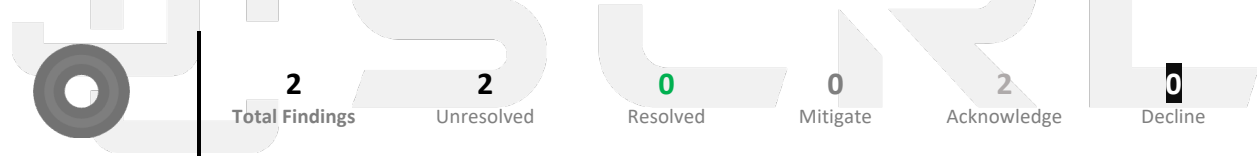
For this security assessment, SCRL received a request on Saturday, January 11, 2025

Client	Language	Audit Method	Confidential	Network Chain	Contract
Cryptosurance	Rust	Automated Analysis (No Code)	Public	Solana	9woD8zJZcTfBxSt6NpJBvCHNRRdDYque2299AntvaPoB
Report Version	Twitter	Telegram	Website		
1.1	https://x.com/cryptosurance	https://t.me/boost/cryptosurance	https://cryptosurance.com/		

Scoring:



Vulnerability Summary



▪ 0 Critical

Critical severity is assigned to security vulnerabilities that pose a severe threat to the smart contract and the entire blockchain ecosystem.

▪ 0 High

High-severity issues should be addressed quickly to reduce the risk of exploitation and protect users' funds and data.

▪ 0 Medium

It's essential to fix medium-severity issues in a reasonable timeframe to enhance the overall security of the smart contract.

▪ 0 Low

While low-severity issues can be less urgent, it's still advisable to address them to improve the overall security posture of the smart contract.

▪ 0 Very Low

Very Low severity is used for minor security concerns that have minimal impact and are generally of low risk.

▪ 2 Informational 2 unresolved

Used to categorize security findings that do not pose a direct security threat to the smart contract or its users. Instead, these findings provide additional information, recommendations

▪ 0 Gas-optimization

Suggestions for more efficient algorithms or improvements in gas usage, even if the current code is already secure.

Please note that the security assessment is **not intended as investment advice**. You should study, understand and accept the risk at your own risk. If you buy pre-sale or any tokens, please note that it is your own responsibility and before any interaction, please check the address. If it does not match what we have checked, it means that it is out our scope of security assessment. **We disclaim any liability arising from the loss of your investment. Cryptocurrencies are very risky. You may lose all your money.**

For Automated Analysis on Solana, we use a specialized tool for checking, which does not check the code, but uses an on-chain method to check.

For SPL Token Program on Solana, we check Mint Authority / Freeze Authority / Auto-Freezing Authority / Malicious Metadata, etc.

Audit Version History:

Version	Date	Description
1.0	Sunday, January 12, 2025	Preliminary Report
1.1	Monday, January 13, 2025	Full Audit Report

Audit information:

Request Date	Audit Date	Re-assessment Date
Saturday, January 11, 2025	Monday, January 13, 2025	-

Smart Contract Audit Summary



SCRL has assessed the security of this smart contract.

The results of the security assessment revealed

No Critical Vulnerabilities.


Full Audit Report by SCRL on January 13, 2025



Security Assessment Author

Auditor:	Mark K. Kevin N. Yusheng T.	[Security Researcher Redteam] [Security Researcher Web3 Dev] [Security Researcher Incident Response]
Document Approval:	Ronny C. Chinnakit J.	CTO & Head of Security Researcher CEO & Founder

Digital Sign



ID: DEF2C489-A403-42A7-B004-47C3D8BED878
Digitally signed by <contact@scrl.io>
January 13, 2025 09:35 AM +07

Please note that the security assessment is **not intended as investment advice**. You should study, understand and accept the risk at your own risk. If you buy pre-sale or any tokens, please note that it is your own responsibility and before any interaction, please check the address. If it does not match what we have checked, it means that it is out our scope of security assessment. **We disclaim any liability arising from the loss of your investment. Cryptocurrencies are very risky. You may lose all your money.**

Disclaimer

Regarding this security assessment, there are no guarantees about the security of the program instruction received from the client is hereinafter referred to as “**Source code**”.

And **SCRL** hereinafter referred to as “**Service Provider**”, the **Service Provider** will not be held liable for any legal liability arising from errors in the security assessment. The responsibility will be the responsibility of the **Client**, hereinafter referred to as “**Service User**” and the

Service User agrees not to be held liable to the **service provider** in any case. By contract

Service Provider to conduct security assessments with integrity with professional ethics, and transparency to deliver security assessments to users The **Service Provider** has the right to postpone the delivery of the security assessment. If the security assessment is delayed whether caused by any reason and is not responsible for any delayed security assessments.

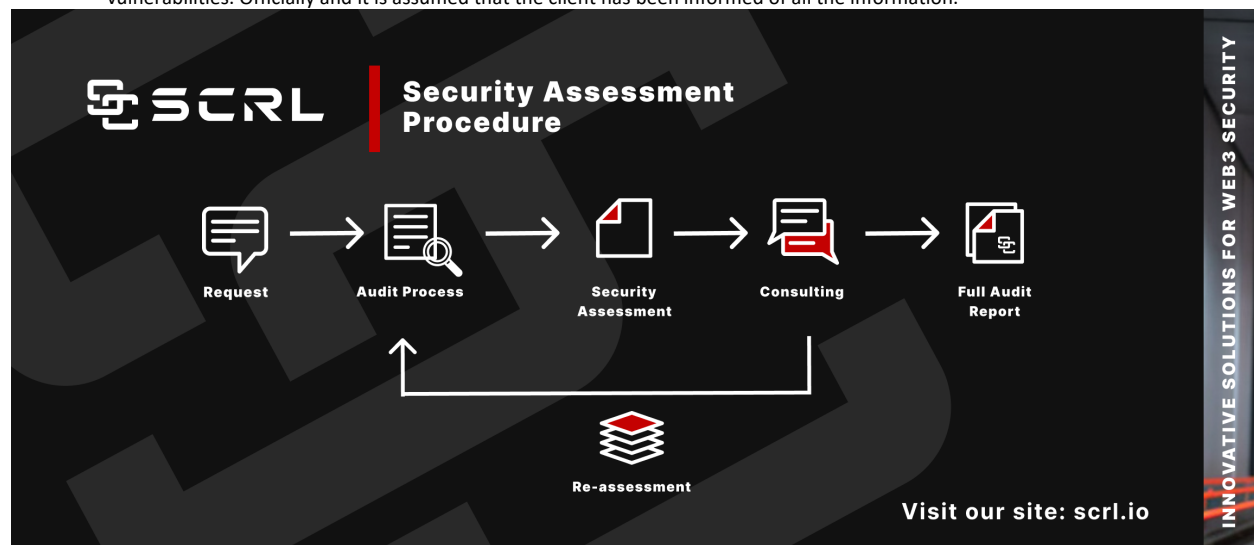
If the **service provider** finds a vulnerability The **service provider** will notify the **service user** via the Preliminary Report, which will be kept confidential for security. The **service provider** disclaims responsibility in the event of any attacks occurring whether before conducting a security assessment. Or happened later All responsibility shall be sole with the **service user**.

Security Assessment Is Not Financial/Investment Advice Any loss arising from any investment in any project is the responsibility of the investor.

SCRL disclaims any liability incurred. Whether it's Rugpull, Abandonment, Soft Rugpull, Exploit, Exit Scam.

Security Assessment Procedure

1. **Request** The client must submit a formal request and follow the procedure. By submitting the source code and agreeing to the terms of service.
2. **Audit Process** Check for vulnerabilities and vulnerabilities from source code obtained by experts using formal verification methods, including using powerful tools such as Static Analysis, SWC Registry, Dynamic Security Analysis, Automated Security Tools, CWE, Syntax & Parameter Check with AI ,WAS (Warning Avoidance System a python script tools powered by SCRL).
3. **Security Assessment** Deliver Preliminary Security Assessment to clients to acknowledge the risks and vulnerabilities.
4. **Consulting** Discuss on risks and vulnerabilities encountered by clients to apply to their source code to mitigate risks.
 - a. **Re-assessment** Reassess the security when the client implements the source code improvements and if the client is satisfied with the results of the audit. We will proceed to the next step.
5. **Full Audit Report** SCRL provides clients with official security assessment reports informing them of risks and vulnerabilities. Officially and it is assumed that the client has been informed of all the information.



Please note that the security assessment is **not intended as investment advice**. You should study, understand and accept the risk at your own risk. If you buy pre-sale or any tokens, please note that it is your own responsibility and before any interaction, please check the address. If it does not match what we have checked, it means that it is out our scope of security assessment. **We disclaim any liability arising from the loss of your investment. Cryptocurrencies are very risky. You may lose all your money.**

Risk Rating

Risk rating using this commonly defined: $Risk\ rating = impact * confidence$

Impact The severity and potential impact of an attacker attack
Confidence Ensuring that attackers expose and use this vulnerability

Confidence	Low	Medium	High
Impact [Likelihood]			
Low	Very Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	Critical

Severity is a risk assessment It is calculated from the Impact and Confidence values using the following calculation methods,

$Risk\ rating = impact * confidence$

It is categorized into

7 categories severity based



For **Informational & Non-class/Optimization/Best-practices** will not be counted as severity

Category

Centralization Centralization Risk is The risk incurred by a sole proprietor, such as the Owner being able to change something without permission	Economics Risk Risks that may affect the economic mechanism system, such as the ability to increase Mint token	Logical Issue Logical Issue is that can cause errors to core processing, such as any prior operations that cause background processes to crash.	Authorization Authorization is Possible pitfalls from weak coding allows unrelated people to take any action to modify the values.	Mathematical Mathematical Any erroneous arithmetic operations affect the operation of the system or lead to erroneous values.	Naming Conventions Naming Conventions naming variables that may affect code understanding or naming inconsistencies
Security Risk Security Risk of loss or damage if it's no mitigate	Coding Style Coding Style is Tips coding for efficiency performance	Best Practices Best Practices is suggestions for improvement	Optimization Optimization is performance improvement	Gas Optimization Gas Optimization is increase performance to avoid expensive gas	Dead Code Dead Code having unused code This may result in wasted resources and gas fees.

Table Of Content

Summary

- Executive Summary
- Scoring
- Vulnerability Summary
- Audit Version History
- Audit Information
- Audit Summary
- Security Assessment Author
- Digital Sign
- Disclaimer
- Security Assessment Procedure
- Risk Rating
- Category

Source Code Detail

- On-chain / Automated Analysis

Vulnerability Finding

- Vulnerability

About SCRL

On-chain / Automated Analysis

Program	SPL Token Program
Checker Date	Sunday, 12 January, 2025
Freeze Authority	No
Mint Authority	No
Metadata Mutable	<u>Yes</u>
Custom Fee	No
Token Contract Address	9woD8zJZcTfBxSt6NpJBvCHNRRdDYque2299AntvaPoB
Contract Creator	3XVyAigrBq1dtNPR3nRHBSErifaxYe7aVNft7XA7ZKNZA

Freeze Authority

The ability to freeze any account, which if used will result in those accounts being unable to process transactions for token holders.

Mint Authority

The ability to continue to mint tokens if they are still in use will negatively impact the ecosystem, potentially increasing the supply of tokens and potentially increasing investor risk.

Metadata Mutable

The ability to edit and change metadata such as name, image, website, and token symbol. If changes occur suddenly without prior notification to the community project, it will affect the credibility of the project.

Custom Fee

Ability to set Custom Fee if setting, which will result in calculation of Fee such as Transfer Fee, Staking/Unstaking Fee, Platform Fee. In general, SPL Token Program does not have a Custom Fee setting.

Please note that the security assessment is **not intended as investment advice**. You should study, understand and accept the risk at your own risk. If you buy pre-sale or any tokens, please note that it is your own responsibility and before any interaction, please check the address. If it does not match what we have checked, it means that it is beyond our scope of security assessment. **We disclaim any liability arising from the loss of your investment. Cryptocurrencies are very risky. You may lose all your money.**

Vulnerability Findings

ID	Vulnerability Detail	Severity	Category	Status
CEN-01	Centralization Risk (Token Distribution)	Informational	Centralization	Acknowledge
MDA-01	Mutable Metadata	Informational	Best Practices	Acknowledge



Please note that the security assessment is **not intended as investment advice**. You should study, understand and accept the risk at your own risk. If you buy pre-sale or any tokens, please note that it is your own responsibility and before any interaction, **please check the smart contract address**. If it does not match what we have checked, it means that it is beyond our scope of security assessment. We disclaim any liability arising from the loss of your investment.
Cryptocurrencies are very risky. You may lose all your money.

CEN-01: Centralization Risk (Token Distribution)

Vulnerability Detail	Severity	Location	Category	Status
Centralization Risk (Token Distribution)	Informational	Check on finding	Centralization	Acknowledge

Finding:

Despite the Token Contract **not containing any malicious functions** that can be executed by the Owner, But, it has been identified that token contracts do not adequately define token distribution, with only one token holder **owning 98.99% as of Sunday, January 12, 2025**. This presents a significant risk of centralization, and all potential participants must give careful consideration to this matter.

We strongly urge all participants **always promptly to verify token holdings** at <https://solscan.io/token/9woD8zJZcTfBxSt6NpJBvCHNRRdDYque2299AntvaPoB#holders>

Address	Quantity	Percentage
3XVyAigrBq1dtNPR3nRHBSErifiYe7aVNf7XA7ZKNZA (Token Owner)	9,899,999,000.00	98.99%
GV7ArwcpdvjcyWPYU4QDkACzoMnuV7JDMRu3Y5GMCMm	100,000,000.00	1.00%
2vGTodWgysPbycmuiiDfYDqdBjJ965vWtp2EmCHQEphR	1,000.00	~0.00%

***Note: Please note that SCRL is not responsible for any investments. And this document is not an investment recommendation document. If any project is in the pre-sale stage, please participate it at your own risk.

https://chat.scr.io/hc/scr-help-center/articles/1717548722-understand-the-risk-of-de_fi-web3

Please note that the security assessment is **not intended as investment advice**. You should study, understand and accept the risk at your own risk. If you buy pre-sale or any tokens, please note that it is your own responsibility and before any interaction, **please check the smart contract address**. If it does not match what we have checked, it means that it is beyond our scope of security assessment. We disclaim any liability arising from the loss of your investment.
Cryptocurrencies are very risky. You may lose all your money.

Recommendation:

We recommend implementing liquidity locks to reduce risks related to token distribution.

Alleviation:

12 Jan 2024 20:04 UTC+7 Cryptsurance: The project is on token presale and not listed on exchanges yet, which is why most of the supply is in 1 wallet. Once the presale is over, it will be distributed to investor wallets and listed exchanges.



Please note that the security assessment is **not intended as investment advice**. You should study, understand and accept the risk at your own risk. If you buy pre-sale or any tokens, please note that it is your own responsibility and before any interaction, **please check the smart contract address**. If it does not match what we have checked, it means that it is beyond our scope of security assessment. We disclaim any liability arising from the loss of your investment.
Cryptocurrencies are very risky. You may lose all your money.

MDA-01: Mutable Metadata

Vulnerability Detail	Severity	Location	Category	Status
Mutable Metadata	Informational	Check on finding	Best Practices	Acknowledge

Finding:

The ability to edit and change metadata such as name, image, website, and token symbol. If changes occur suddenly without prior notification to the community project, it will affect the credibility of the project.

```
{  
  "isMutable": 1,  
}
```

Recommendation:

Ensuring your token's immutability is essential for maintaining its security and stability. Revoking the update authority eliminates the possibility of future modifications, protecting the token's integrity and preventing potential confusion among holders.

Alleviation: -

Please note that the security assessment is **not intended as investment advice**. You should study, understand and accept the risk at your own risk. If you buy pre-sale or any tokens, please note that it is your own responsibility and before any interaction, **please check the smart contract address**. If it does not match what we have checked, it means that it is beyond our scope of security assessment. We disclaim any liability arising from the loss of your investment.
Cryptocurrencies are very risky. You may lose all your money.

About SCRL

SCRL (Previously name SECURI LAB) was established in 2020, and its goal is to deliver a security solution for Web3 projects by expert security researchers. To verify the security of smart contracts, they have developed internal tools and KYC solutions for Web3 projects using industry-standard technology. SCRL was created to solve security problems for Web3 projects. They focus on technology for conciseness in security auditing. They have developed Python-based tools for their internal use called WAS and SCRL. Their goal is to drive the crypto industry in Thailand to grow with security protection technology.



Support ALL EVM L1 - L2

Smart Contract Audit

Our top-tier security strategy combines static analysis, fuzzing, and a custom detector for maximum efficiency.

scrl.io



Follow Us On:

Website	https://scrl.io/
Twitter	https://twitter.com/scrl_io
Telegram	https://t.me/scrl_io
Medium	https://scrl.medium.com/

Please note that the security assessment is **not intended as investment advice**. You should study, understand and accept the risk at your own risk. If you buy pre-sale or any tokens, please note that it is your own responsibility and before any interaction, **please check the smart contract address**. If it does not match what we have checked, it means that it is beyond our scope of security assessment. We disclaim any liability arising from the loss of your investment.
Cryptocurrencies are very risky. You may lose all your money.