www.sooho.io



LumiWave

# SECURITY ASSESSMENT REPORT

FINAL

Token & Vote Contract

**Ver_1.0**

2024.05.09

# 1. Executive Overview

## 1-1. Abstract

**LumiWave is a token based on Sui.** It allows users to execute transactions quickly at a low cost.

SOOHO Audit conducted a security audit of the LumiWave Token & Vote Contract for a period of 15 days, **from April 24, 2024, to May 9, 2024**. This security audit aims to **detect security threats such as functional errors** in the token and vote contract, which is a core implementation for LumiWave.

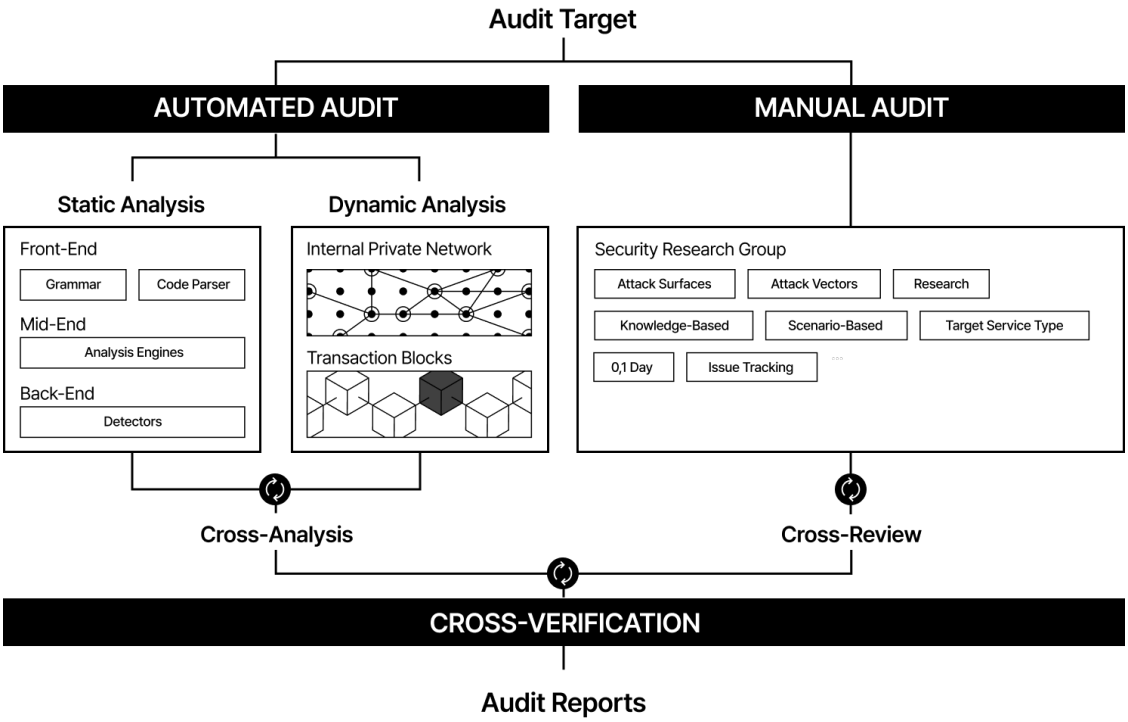
As a result, SOOHO Audit discovered **a total of 1 issue**. Note that **1 of 0** issues have been resolved by the LumiWave team. Through this audit, we have successfully addressed several threats, but it is important to note that the verification was limited to the essential aspects necessary to achieve the audit's objectives within the given resources. We recommend continuous security audits to consistently enhance the project's safety.

# 1-2. Assessment Methodology

SOOHO Audit applies two audit methodologies, Automated Audit and Manual Audit, to conduct a more comprehensive blockchain security audit.

Automated Audit utilizes cooperative analysis between static analysis and dynamic analysis to accurately and quickly detect various attacks, ensuring a high-quality audit. SOOHO's proprietary analyzer performs static analysis by parsing the syntax of the client's contract code, conducting semantic inference, variable tracking, and path exploration to validate conditions. In static analysis, SOOHO performs more sophisticated analysis through actual operation analysis, fuzzing, and concolic execution in its own test network.

In Manual Audit, SOOHO's team of security audit experts directly verifies the client's project by leveraging various security and domain knowledge. They focus on analyzing code with higher risks and examine whether the code has been written as intended by the partner company and whether access management is functioning correctly. Security audit experts handle complex attack scenarios and recent security issues, complementing the automated analysis to enhance the completeness of the audit. Additionally, through cross-validation among experts, more refined security audit results are provided.



SOOHO.IO

# SOOHO.IO Audit Certificate

SOOHO.IO Verified on May 9, 2024

## Project Overview

| | | | |
|---|---|---|---|
| **Chain** | Sui | **Language** | Move |
| **# of Files** | 4 | **# of Lines** | 437 |
| **Repository** | https://github.com/LumiWave/inno-contract | | |
| **Commit** | 2b990663682bf41e26dcb1e07ec6891bd263c47b | | |
| **Audit Period** | April 24, 2024 - May 9, 2024 | | |

## Findings Overview

| Found | Resolved | Partially Resolved | Acknowledged |
|---|---|---|---|
| 1 | 0 | 0 | 0 |

| | |
|---|---|
| CRITICAL | 0 |
| HIGH | 0 |
| MEDIUM | 0 |
| LOW | 1 |
| NOTE | 0 |

# Revision History

- Ver_1.0 - Issued on May 9, 2024 : Initial Submission

# 2. Audit Summary

## 2-1. Findings Summary

| Issue ID | Severity | Description | Status |
|---|---|---|---|
| VLS-SDS-001 | LOW | Possible DoS in `vote::vote_counting` | Found |

## 2-2. Verification Summary

| Verification ID | Description | Status |
|---|---|---|
| OnlyVoteCanMint | After the initial mint, additional mint is only possible through voting. | **Verified** |
| DenyCapAvail | add_deny can block token transfers. | **Verified** |
| CoinLockable | Token can be locked and transfered to a wallet. | **Verified** |

# 3. Findings

## #1. Possible DoS in vote::vote_counting

| Status | Found | Issue ID | VLS-SDS-001 |
|---|---|---|---|
| Issue Type | Denial of Service | Severity | LOW |
| Files affected | /sources/vote.move | | |

```
1          while( i < vector::length(&participants)) {
2              let participant = vector::borrow(&participants, i);
3              if ( participant.is_agree == true ) {
4                  agree_cnt = agree_cnt + 1;
5              }else{
6                  disagree_cnt = disagree_cnt + 1;
7              };
8              i = i + 1;
```

https://github.com/LumiWave/inno-contract/blob/2b990663682bf41e26dcb1e07ec6891bd263c47b/LUMIWAVE/sources/vote.move#L113-L120

### Details

vote::vote_counting aggregates the results of completed votes. If an unusually high number of wallets participate in a specific vote, the transaction may fail due to exceeding the execution limit. This could be exploited by malicious users to continuously cause the failure of vote counting intended for additional minting.

### Mitigation

Instead of aggregating the vote results through a final loop, it is recommended to implement a loop-free structure by saving the vote count after each vote function.

# 4. Appendix

## 4-1. Severity Definitions

| | |
|---|---|
| CRITICAL | There is a clear potential for **direct asset leakage** or **immediate system shutdown** in a typical environment. |
| HIGH | There is a clear potential for **indirect asset leakage** or **system disruption** in a typical environment. |
| MEDIUM | There is a possibility of **temporary system suspension** in typical environment or **potential asset exposure** in highly specific situations. |
| LOW | There is a potential for **temporary system suspension** or **partial functionality impairment** in highly specific situations. |
| NOTE | It is recommended for **functional optimization**. |

## 4-2. File Hash Calculation Method

In the "Checksum" field of the "Audit Scope" section, the SHA-256 (Secure Hash Algorithm 2) digest, with a digest size of 256 bits, is used to calculate the checksum. It represents the hash value of each file content hosted in the specified source repositories listed below the designated commit. The result is encoded in hexadecimal format and is equivalent to the output of the Linux "shasum" command for the target files.

## 4-3. Vulnerability Classification

| | |
|---|---|
| **Access Control** | When permissions are not properly granted to functions that should have authorization, or when arbitrary users can access privileged functions. |
| **Authentication** | When a user has the ability to influence values associated with arbitrary other EOAs or CAs. |
| **Data Validation** | When there is a lack of appropriate validation for the data provided by the user or when trusting unreliable data. |
| **Reentrancy** | When there is a presence of reentrancy vulnerability. |
| **Centralization** | When the permissions of the Owner or Admin are excessively strong, leading to the potential for a rug-pull. |
| **Misimplementation** | When there is a specification in the documentation, but the implementation is flawed, resulting in unintended or incorrect functionality. |
| **Undefined Behavior** | In specific cases where unforeseen scenarios in the design lead to unintended outcomes. |
| **Deprecated Code** | When using outdated versions of the code that require patching. |
| **Front-running** | When there is a loss of value due to front-running. |
| **Gas Optimization** | When there are opportunities to optimize gas usage. |
| **Bad Randomness** | When using a predictable random function. |
| **Oracle Security** | When using an incorrect Price Oracle or misusing the Oracle libraries. |
| **Denial of Service** | When there is a potential for a Denial of Service (DoS) attack. |
| **Timing** | When vulnerabilities occur based on the order or timing of transactions. |
| **Cryptography** | When vulnerabilities are associated with cryptographic basis. |
| **Best Practice** | Conventional best practices for producing high-quality code. |

# 4-4. Audit Scope

| Filename | SHA1 Hash |
| --- | --- |
| Move.toml | 0c834c31f2386f7c6fa94032a5382da34fcd9c04 |
| sources/lock_coin.move | 1ae68d31c644856974e8fddf8bed54c18a0fec0e |
| sources/lumiwave.move | 740f11441c27d628e77242c9d7c53ea6ec3b2cce |
| sources/vote.move | 37551a9941118519356bf91c6553158473d16240 |

## About SOOHO.IO

SOOHO started with the aim of researching and providing technologies to enhance the security and reliability of the blockchain ecosystem. SOOHO verifies smart contract vulnerabilities using its own vulnerability analyzer and open-source analyzers. In addition, SOOHO's security team consists of skilled professionals with excellent hacking capabilities and experience, including winning awards in hacking competitions such as Defcon, Nuit du Hack, White Hat, SamsungCTF, and having academic backgrounds such as doctoral degrees in security. The experts at SOOHO are dedicated to protecting clients' smart contracts from both known 1-DAY vulnerabilities and 0-DAY vulnerabilities.

## Contact us

Twitter @SOOHO_AUDIT
E-mail audit@sooho.io
Website https://www.sooho.io/solution/audit/





# Disclaimer

This report is subject to the terms and conditions specified in the service agreement (including but not limited to service descriptions, confidentiality, disclaimers, and liability limitations) or the terms and conditions applicable to the services provided to you ("Customer" or "Company") in relation to the contract. The report provided regarding the services specified in this agreement can only be used by the Company within the scope permitted by the terms specified in this agreement. This report cannot be transmitted, disclosed, referenced, or relied upon by any party other than the Company for any purpose without the prior written consent of SOOHO.IO, nor can copies be provided without such consent. This report is not intended to "approve" or "disapprove" of any specific project or team, nor should it be considered as such. This report does not represent the economic viability or value of any "products" or "assets" created by the team or project that has contracted with SOOHO.IO to perform security assessments, nor should it be considered as such. This report does not provide any guarantee or assurance of absolute bug integrity of the analyzed technology, nor does it provide any representation regarding technology ownership, business, business models, or legal compliance. This report should not be used in any way to make investment or participation decisions regarding a specific project.

This report does not provide investment advice and should not be used as any form of investment advice. This report represents a comprehensive evaluation process to help customers improve the quality of their code and reduce the high level of risks associated with cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets inherently carry a high level of ongoing risks. SOOHO.IO's position is that each company and individual has their own responsibility for conducting their own due diligence and maintaining ongoing security. The goal of SOOHO.IO is to assist in reducing high levels of variance and attack vectors associated with the utilization of constantly evolving new technologies and does not claim any guarantee of the security or functionality of the analyzed technology. The evaluation services provided by SOOHO.IO are subject to dependencies and are under continuous development. By accessing and/or using the services, reports, and materials, you agree that you assume full responsibility for your access to and/or use of them as is, as available. Cryptographic tokens are an emerging technology and carry a high level of technical risks and uncertainties. Evaluation reports may include false positives, false negatives, and other unpredictable results.

www.sooho.io



# Institutional-Grade DeFi Infrastructure

To invite anyone who wishes to expand their financial opportunities, SOOHO is building a transparent and secure infrastructure with reliable partners. We aim to establish a cross-chain ecosystem connected by the safest bridges, creating a Gateway that enables easy access to various financial opportunities.