SolidityScan | Powered by CRED SHIELDS

# Security Assessment Report

## HelioCoin

22 July 2025

This security assessment report was prepared by SolidityScan.com, a cloud-based Smart Contract Scanner.

# Table of Contents

| |
|---|
| REVERT STATEMENTS WITHIN EXTERNAL AND PUBLIC FUNCTIONS CAN BE USED TO PERFORM DOS ATTACKS |
| USE SCIENTIFIC NOTATION |
| ARRAY LENGTH CACHING |
| AVOID RE-STORING VALUES |
| AVOID ZERO-TO-ONE STORAGE WRITES |
| CHEAPER INEQUALITIES IN IF() |
| CHEAPER INEQUALITIES IN REQUIRE() |
| DEFAULT INT VALUES ARE MANUALLY RESET |
| DEFINE CONSTRUCTOR AS PAYABLE |
| FUNCTIONS CAN BE IN-LINED |
| REVERTING FUNCTIONS CAN BE PAYABLE |
| GAS OPTIMIZATION IN INCREMENTS |
| INTERNAL FUNCTIONS NEVER USED |
| OPTIMIZING ADDRESS ID MAPPING |
| STORAGE VARIABLE CACHING IN MEMORY |
| UNNECESSARY CHECKED ARITHMETIC IN LOOP |

## 05 Scan History

## 06 Disclaimer

# 01. Vulnerability Classification and Severity

## Description

To enhance navigability, the document is organized in descending order of severity for easy reference. Issues are categorized as *Fixed*, *Pending Fix*, or *Won't Fix*, indicating their current status. *Won't Fix* denotes that the team is aware of the issue but has chosen not to resolve it. Issues labeled as *Pending Fix* state that the bug is yet to be resolved. Additionally, each issue's severity is assessed based on the risk of exploitation or the potential for other unexpected or unsafe behavior.

### Critical

The issue affects the contract in such a way that funds may be lost, allocated incorrectly, or otherwise result in a significant loss.

### High

High-severity vulnerabilities pose a significant risk to both the Smart Contract and the organization. They can lead to user fund losses, may have conditional requirements, and are challenging to exploit.

### Medium

The issue affects the ability of the contract to operate in a way that doesn't significantly hinder its behavior.

### Low

The issue has minimal impact on the contract's ability to operate.

### Informational

The issue does not affect the contract's operational capability but is considered good practice to address.

### Gas

This category deals with optimizing code and refactoring to conserve gas.

# 02. Executive Summary

**HelioCoin**

0×2A0c1070025391ddb789E69392aB3E9256B0F7d0

https://polygonscan.com/address/0×2A0c1070025391ddb789E...

| Language | Audit Methodology | Contract Type |
|---|---|---|
| **Solidity** | **Static Scanning** | - |

| Website | Publishers/Owner Name | Organization |
|---|---|---|
| - | - | - |

Contact Email

-


## Security Score is GREAT

The SolidityScan score is calculated based on lines of code and weights assigned to each issue depending on the severity and confidence. To improve your score, view the detailed result and leverage the remediation solutions provided.

This report has been prepared for HelioCoin using SolidityScan to scan and discover vulnerabilities and safe coding practices in their smart contract including the libraries used by the contract that are not officially recognized. The SolidityScan tool runs a comprehensive static analysis on the Solidity code and finds vulnerabilities ranging from minor gas optimizations to major vulnerabilities leading to the loss of funds. The coverage scope pays attention to all the informational and critical vulnerabilities with over 450+ modules. The scanning and auditing process covers the following areas:

Various common and uncommon attack vectors will be investigated to ensure that the smart contracts are secure from malicious actors. The scanner modules find and flag issues related to Gas optimizations that help in reducing the overall Gas cost It scans and evaluates the codebase against industry best practices and standards to ensure compliance It makes sure that the officially recognized libraries used in the code are secure and up to date.

The SolidityScan Team recommends running regular audit scans to identify any vulnerabilities that are introduced after HelioCoin introduces new features or refactors the code.

# 03. Threat Summary

Threat Score


High Risk

**32.5**/100

## THREAT SUMMARY

Your smart contract has been assessed and assigned a **High Risk** threat score. The score indicates the likelihood of risk associated with the contract code.

### Contract's source code is verified.

Source code verification provides transparency for users interacting with smart contracts. Block explorers validate the compiled code with the one on the blockchain. This also gives users a chance to audit the contracts, ensuring that the deployed code matches the intended functionality and minimizing the risk of malicious or erroneous contracts.

### The contract can mint new tokens.

Minting functions are often utilized to generate new tokens, which can be allocated to specific addresses, such as user wallets or the contract owner's wallet. This feature is commonly employed in various decentralized finance (DeFi) and non-fungible token (NFT) projects to facilitate token issuance and distribution. The Presence of Minting Function module is designed to quickly identify the presence and implementation of minting functions in a smart contract. Mint functions play a crucial role in creating new tokens and transferring them to the designated user's or owner's wallet. This process significantly contributes to increasing the overall circulation of the tokens within the ecosystem.

### The tokens can be burned in this contract.

The token contract incorporates a burn function that enables the intentional reduction of token amounts, consequently diminishing the total supply. The execution of this burn function contributes to the creation of scarcity within the token ecosystem, as the overall availability of the token decreases.

### The contract can be compiled with a more recent Solidity version

The contract should be written using the latest Solidity pragma version as it comes with numerous bug fixes. Utilizing an outdated version exposes the contract to vulnerabilities associated with known issues that have been addressed in subsequent updates. Therefore, it is essential to stay current with the latest Solidity version to ensure the robustness and security of the contract against potential vulnerabilities.

---

### This is not a proxy-based upgradable contract.

The Proxy-Based Upgradable Contract module is dedicated to identifying the presence of upgradeable contracts or proxy patterns within a smart contract. The utilization of upgradeable contracts or proxy patterns enables contract owners to make dynamic changes to various aspects, including functions, token circulation, and distribution, without requiring a complete redeployment of the contract.

---

### Owners can blacklist tokens or users.

This module is designed to identify whether the owner of a smart contract has the capability to blacklist specific tokens or users. In a scenario where owners possess the authority to blacklist, all transactions related to the blacklisted entities will be immediately halted. Ownership privileges that include the ability to blacklist tokens or users can be a critical feature in certain use cases, providing the owner with control over potential malicious activities, compliance issues, or other concerns. However, in situations where this authority is abused or misapplied, it can lead to unintended consequences and user dissatisfaction.

---

### Is ERC-20 token.

A token is expected to adhere to the established standards of the ERC-20 token specification, encompassing the inclusion of all necessary functions with standardized names and arguments as defined by the ERC-20 standard.

---

### This is a Pausable contract.

Pausable contracts refer to contracts that can be intentionally halted by their owners, temporarily preventing token holders from engaging in buying or selling activities. This pause mechanism allows contract owners to exert control over the token's functionality, introducing a temporary suspension in trading activities for various reasons such as security concerns, updates, or regulatory compliance adjustments.

---

### Critical functions that add, update, or delete owner/admin addresses are not detected.

A smart contract within the Web3 ecosystem that incorporates critical administrative functions can potentially compromise the transparency and intended objectives of the contract. It is imperative to conduct a thorough examination of these functions, especially in the realm of Web3 smart contracts. Minimizing administrative functions in a token contract within the Web3 framework can significantly reduce the likelihood of complications and enhance overall efficiency and clarity.

---

### The contract cannot be self-destructed by owners.

The SELFDESTRUCT opcode is a critical operation in Ethereum smart contracts, allowing a contract to autonomously terminate itself. When invoked, this opcode deallocates the contract, freeing up storage and computational resources on the Ethereum blockchain. Notably, the remaining Ether in the contract is sent to a specified address, ensuring a responsible handling of funds.

---

### The contract is vulnerable to ERC-20 approve Race condition vulnerability.

The ERC-20 race condition arises when two or more transactions attempt to interact with the same ERC-20 token contract concurrently. This scenario can result in conflicts and unexpected behavior due to the non-atomic nature of certain operations in the contract. Atomicity refers to the concept that an operation is indivisible and occurs as a single, uninterruptible unit.

---

### The contract's owner was found.

Renounced ownership indicates that the contract is truly decentralized, as the owner has relinquished control, ensuring that the contract's functionality and rules cannot be altered by administrators or any central authority.

---

### Addresses contain more than 20% of circulating token supply.

Users with token balances exceeding 5% of the circulating token supply are critical to monitor, as their actions can significantly influence the token's price and ecosystem. Proper token distribution helps maintain a healthy market by preventing concentration of power and promoting fair participation.

---

### The contracts are using functions that can only be called by the owners.

An overpowered owner risk occurs when a contract has numerous functions that only the owner can execute. This can lead to centralization issues and potential abuse, as the owner has disproportionate control over the contract's operations.

---

### The contract does not have a cooldown feature.

Cooldown functions, a crucial aspect in the smart contract landscape, are employed to temporarily suspend trading activities or other contract workflows. The mechanism introduces a time-based delay, effectively preventing users from repeatedly executing transactions or engaging in rapid buying and selling of tokens. Cooldown functions are used to halt trading or other contract workflows for a certain amount of time so as to prevent users from repeatedly executing transactions or buying and selling tokens.

---

### Owners cannot whitelist tokens or users.

This empowers the contract owner to selectively grant privileges to users, such as exemption from fees or access to unique contract features.

---

### Owners cannot set or update Fees in the contract.

In the context of smart contracts, fees are essential components that may be associated with various functionalities, such as transactions, token transfers, or other specific actions. The ability for owners to set or update fees is particularly valuable in scenarios where fee adjustments are needed to align with market conditions, regulatory requirements, or project-specific considerations. The Owners Can Set or Update Fees module focuses on identifying the capability within a smart contract for owners to establish or modify fees. This feature allows contract owners to have control over the fee structure within the contract, providing flexibility and adaptability to changing circumstances.

---

### Hardcoded addresses were not found.

The inclusion of a fixed or hardcoded address within a smart contract has the potential to pose significant challenges in the future, particularly concerning the contract's adaptability and upgradability. This static reference to an address may impede the seamless implementation of updates or modifications to the contract, hindering its ability to evolve in response to changing requirements. Such rigidity may result in complications and obstacles when attempting to enhance or alter the smart contract's functionality over time.

---

### The contract does not have any owner-controlled functions modifying token balances.

The Owners Updating Token Balance module is focused on identifying situations where a smart contract has functions controlled by owners that allow them to update token balances for other users or the contract. If a contract permits owners to manipulate token balances, it can have significant implications on user holdings and overall contract integrity. In some scenarios, contracts may provide owners with functions that enable the manual adjustment of token balances. While this feature can be legitimate for specific use cases, such as token distribution or rewards, it also introduces potential risks. Allowing owners to arbitrarily update token balances may lead to vulnerabilities, manipulation, or unintended changes in the token ecosystem.

---

### Owner's wallet contains 978998063.7481164 tokens which is more than 97.9% of the circulating token supply.

A check on the owner's wallet balance exceeding a specific token amount can indicate a centralization risk, where the owner may have disproportionate control over the token supply, potentially leading to manipulation or abuse.

---

### No such functions retrieving ownership were found.

The Function Retrieving Ownership module serves the purpose of swiftly and efficiently retrieving ownership-related information within a smart contract. This functionality is vital for projects seeking to access and manage ownership data seamlessly. Utilizing this module, developers can streamline the process of obtaining ownership details, contributing to the effective administration of ownership-related functions within the ecosystem.

---

### IS SPAM CONTRACT

A spam NFT is an NFT that is considered low-quality or deceptive, cluttering the marketplace and potentially misleading users.

---

### Absence of Malicious Typecasting.

Malicious typecasting, particularly the conversion of uint160 values to addresses, is a tactic often used by scammers to create deceptive addresses that can bypass standard detection mechanisms, facilitating fraudulent activities.

---

## LIQUIDITY BURN STATUS

The liquidity burn status indicates whether the LP tokens for the scanned contract have been permanently removed or remain accessible. If burnt, the LP tokens are sent to an irrecoverable address, ensuring that the liquidity cannot be withdrawn, offering permanent stability and security to the project. If not burnt, the LP tokens could still be accessed and withdrawn, which might expose investors to risks of liquidity manipulation or removal.

## LIQUIDITY LOCK STATUS

The liquidity status determines whether the liquidity for the scanned contract is securely locked or accessible. If locked, LP tokens are stored in a time-locked contract, preventing any withdrawals until the lock expires. This helps protect investors from sudden liquidity removal. If not locked, LP tokens remain accessible, allowing project developers or liquidity providers to withdraw liquidity at any time, potentially posing risks to investors.

## No such functions having totalSupply function update were found.

A fixed supply token is critical when the token's value is tied to scarcity or when precise control over inflation or deflation is required. Without a fixed supply, the contract could introduce unexpected inflation, devalue the token, or erode trust in the token's consistency.

## No such functions having gas abuse via malicious minting.

Gas abuse refers to patterns within smart contracts that manipulate gas consumption in ways that unnecessarily increase transaction costs for users. This can occur through various mechanisms designed to exploit gas inefficiencies or inflate gas usage, shifting the financial burden onto users without their knowledge.

## Valid token name or symbol.

The token name or symbol contains potentially harmful content, such as HTML tags or JavaScript code. If these unsanitized strings are displayed by user interfaces, they could execute scripts in users' browsers, posing a significant risk of Cross-Site Scripting (XSS).

### No such functions having addresses with special access.

Special permissions granted to non-owner addresses allow them to execute specific functions with elevated access. This can introduce security risks, as these privileged addresses may perform critical operations that impact the contract's state or user funds. If not properly managed or monitored, these permissions could lead to unauthorized or malicious actions, compromising the contract's integrity.

### No hidden owner detected

The Hidden Owner check identifies whether there are any hidden owner roles within the contract. Hidden ownership can allow unauthorized access and control over contract functions, which poses a risk to users and stakeholders.

### COUNTERFEIT TOKEN

The contract is found to have the token symbol identical to that of official tokens, thereby falling under the category of counterfeit tokens. These counterfeit tokens can mislead users into believing they are interacting with legitimate, well-known cryptocurrencies, potentially leading to financial losses and damaging the reputation of the official token.

### Absence of external call risk in critical functions.

This check identifies risks associated with external calls within critical functions. External calls can introduce vulnerabilities such as unexpected state changes, or dependencies on external contracts, which may compromise the integrity and reliability of the function’s execution.

### Antiwhale Simulation - Token Lacks Antiwhale Measures

The simulation for the scanned contract indicates that this token does not incorporate antiwhale measures. Large holders may have significant impacts on the market, which could lead to potential volatility.

### Optimal sell fee.

The sell fee is 5% or less, keeping transaction costs low and making the token more appealing for trading and long-term holding.

### Token Sell Simulation - Successful!

The token sell simulation for the scanned contract was completed successfully! The transaction went through smoothly, and we did not detect any unusual patterns or honeypot behavior. This confirms that the contract supports token sales effectively, with no signs of malicious activity. The total tax for the sell transaction is `0.0%`, and the gas used in the transaction is `36374.0`

---

### Token Transfer Simulation - Successful!

The token transfer simulation for the scanned contract was successful! The tokens were transferred to the designated recipient without any issues, and we did not detect any unusual patterns or honeypot tactics. This positive result ensures that the contract allows for seamless token transfers with no hidden risks.

---

### Optimal buy fee

The buy fee is below 5%, keeping transaction costs low and making the token more appealing for trading and long-term engagement.

---

### Token Purchase Simulation - Successful!

The token purchase simulation for the scanned contract was successful! The transaction process was executed perfectly, and we did not detect any unusual patterns or honeypot behavior. This indicates that the contract functions correctly for token purchases, with no signs of fraudulent activity or hidden traps. The total tax for the buy transaction is `0.0%`, and the gas used in the transaction is `64369.0`

Issue Type

**PRESENCE OF MINTING FUNCTION**

Action Taken

*Pending Fix*

Description

Minting functions are often utilized to generate new tokens, which can be allocated to specific addresses, such as user wallets or the contract owner's wallet. This feature is commonly employed in various decentralized finance (DeFi) and non-fungible token (NFT) projects to facilitate token issuance and distribution. The Presence of Minting Function module is designed to quickly identify the presence and implementation of minting functions in a smart contract. Mint functions play a crucial role in creating new tokens and transferring them to the designated user's or owner's wallet. This process significantly contributes to increasing the overall circulation of the tokens within the ecosystem.

---

### Remediation

It is important to ensure the minting function includes proper access control mechanisms to restrict token minting to authorized addresses only, thereby preventing unauthorized or excessive token creation.

| File Location | Line No. |
| --- | --- |
| contract.sol | L940 - L943 |

Issue Type

**PRESENCE OF BURN FUNCTION**

Action Taken

*Pending Fix*

Description

The token contract incorporates a burn function that enables the intentional reduction of token amounts, consequently diminishing the total supply. The execution of this burn function contributes to the creation of scarcity within the token ecosystem, as the overall availability of the token decreases.

---

### Remediation

Consider adding access control modifiers to the burn function to prevent another user from burning their tokens.

| File Location | Line No. |
| --- | --- |
| contract.sol | L947 - L949 |

Issue Type

**SOLIDITY PRAGMA VERSION**

Action Taken

*Pending Fix*

Description

The contract should be written using the latest Solidity pragma version as it comes with numerous bug fixes. Utilizing an outdated version exposes the contract to vulnerabilities associated with known issues that have been addressed in subsequent updates. Therefore, it is essential to stay current with the latest Solidity version to ensure the robustness and security of the contract against potential vulnerabilities.

### Remediation

Update the Solidity pragma version to the latest stable version to benefit from the latest bug fixes and security enhancements.

| File Location | Line No. |
|---|---|
| contract.sol | L8 - L8 |
| contract.sol | L90 - L90 |
| contract.sol | L118 - L118 |
| contract.sol | L148 - L148 |
| contract.sol | L313 - L313 |
| contract.sol | L626 - L626 |
| contract.sol | L728 - L728 |

| File Location | Line No. |
| --- | --- |
| contract.sol | L835 - L835 |

Issue Type

**OWNERS CANNOT BLACKLIST TOKENS OR USERS**

Action Taken

*Pending Fix*

Description

This module is designed to identify whether the owner of a smart contract has the capability to blacklist specific tokens or users. In a scenario where owners possess the authority to blacklist, all transactions related to the blacklisted entities will be immediately halted. Ownership privileges that include the ability to blacklist tokens or users can be a critical feature in certain use cases, providing the owner with control over potential malicious activities, compliance issues, or other concerns. However, in situations where this authority is abused or misapplied, it can lead to unintended consequences and user dissatisfaction.

---

### Remediation

Ensure that ownership privileges do not include the ability to blacklist tokens or users, as this feature can lead to centralization concerns and potential misuse. Instead, implement transparent governance mechanisms for handling compliance issues or malicious activities.

| File Location | Line No. |
| --- | --- |
| contract.sol | L921 - L921 |

Issue Type

**PAUSABLE CONTRACTS**

Action Taken

⚠ *Pending Fix*

Description

Pausable contracts refer to contracts that can be intentionally halted by their owners, temporarily preventing token holders from engaging in buying or selling activities. This pause mechanism allows contract owners to exert control over the token's functionality, introducing a temporary suspension in trading activities for various reasons such as security concerns, updates, or regulatory compliance adjustments.

---

### Remediation

Implement the pause() and unpause() functions in your contract and secure them with the onlyOwner modifier. This ensures that only the contract owner has the authority to change the paused state of the contract. Additionally, verify that the owner is correctly set and that the access control mechanisms are thoroughly tested to prevent any unauthorized actions.

| File Location | Line No. |
|---|---|
| contract.sol | L787 - L789 |
| contract.sol | L787 - L789 |
| contract.sol | L794 - L796 |
| contract.sol | L794 - L796 |
| contract.sol | L801 - L803 |
| contract.sol | L801 - L803 |

| File Location | Line No. |
| --- | --- |
| contract.sol | L812 - L815 |
| contract.sol | L824 - L827 |
| contract.sol | L971 - L973 |
| contract.sol | L976 - L978 |

Issue Type

**ERC20 RACE CONDITION**

Action Taken

⚠ *Pending Fix*

Description

The ERC-20 race condition arises when two or more transactions attempt to interact with the same ERC-20 token contract concurrently. This scenario can result in conflicts and unexpected behavior due to the non-atomic nature of certain operations in the contract. Atomicity refers to the concept that an operation is indivisible and occurs as a single, uninterruptible unit.

### Remediation

Implement locking mechanisms or state variables to ensure that only one transaction can modify the token balances or allowances at a time, thereby preventing the race condition.

| File Location | Line No. |
| --- | --- |
| contract.sol | L434 - L438 |
| contract.sol | L565 - L567 |
| contract.sol | L608 - L618 |

Issue Type

**OVERPOWERED OWNERS**

Action Taken

⚠ *Pending Fix*

Description

An overpowered owner risk occurs when a contract has numerous functions that only the owner can execute. This can lead to centralization issues and potential abuse, as the owner has disproportionate control over the contract's operations.

### Remediation

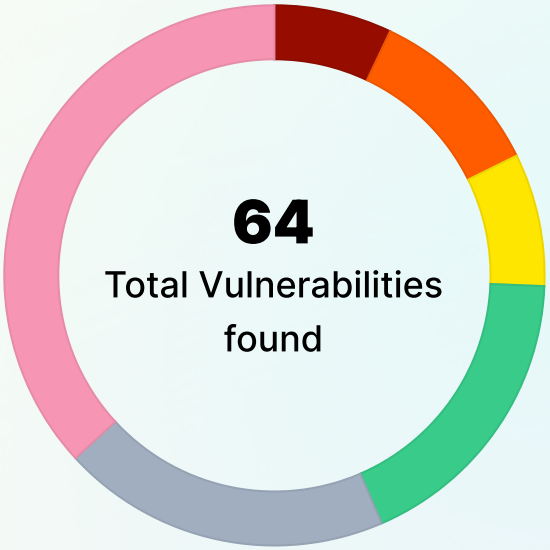
Review and minimize the number of critical functions accessible to owners, ensuring that these functions are necessary for contract management and do not pose undue risk to users' funds in the event of compromise or misuse. Implement multi-signature or governance mechanisms for critical actions to distribute authority and mitigate risk.

| File Location | Line No. |
|---|---|
| contract.sol | L697 - L699 |
| contract.sol | L705 - L710 |
| contract.sol | L940 - L943 |
| contract.sol | L955 - L968 |
| contract.sol | L971 - L973 |
| contract.sol | L976 - L978 |
| contract.sol | L983 - L992 |

# 04. Findings Summary

0×2A0c1070025391ddb789E69392aB3E9256B0F7d0
POLYGON (Polygon Mainnet) | View on Polygonscan

| Security Score | Scan duration | Lines of code |
|---|---|---|
| 89.80/100 | 12 secs | 882 |




| 0 | 4 | 1 | 12 | 14 | 33 |
|---|---|---|---|---|---|
| Crit | High | Med | Low | Info | Gas |

This audit report has not been verified by the SolidityScan team. To learn more about our published reports. click here

## ACTION TAKEN

| 0 | 0 | 0 | 65 |
|---|---|---|---|
| Fixed | False Positive | Won't Fix | Pending Fix |

| S. No. | Severity | Bug Type | Instances | Detection Method | Status |
|---|---|---|---|---|---|
| H001 | High | APPROVE FRONT-RUNNING ATTACK | 3 | Automated | Pending Fix |
| H002 | High | UNCHECKED TRANSFER | 1 | Automated | Pending Fix |
| M001 | Medium | MODIFIER SIDE EFFECTS | 1 | Automated | Pending Fix |
| L001 | Low | USE OF FLOATING PRAGMA | 10 | Automated | Pending Fix |
| L002 | Low | MISSING EVENTS | 2 | Automated | Pending Fix |
| L003 | Low | MISSING ZERO ADDRESS VALIDATION | 3 | Automated | Pending Fix |
| L004 | Low | OUTDATED COMPILER VERSION | 8 | Automated | Pending Fix |
| L005 | Low | USE OWNABLE2STEP | 1 | Automated | Pending Fix |
| I001 | Informational | BLOCK VALUES AS A PROXY FOR TIME | 2 | Automated | Pending Fix |
| I002 | Informational | CONSTRUCTORS SHOULD EMIT AN EVENT | 3 | Automated | Pending Fix |
| I003 | Informational | CONTRACT NAME SHOULD USE PASCALCASE | 1 | Automated | Pending Fix |
| I004 | Informational | IF-STATEMENT REFACTORING | 1 | Automated | Pending Fix |
| I005 | Informational | INTERFACES SHOULD BE DECLARED IN A SEPARATE FILE | 3 | Automated | Pending Fix |
| I006 | Informational | MODIFIER CREATED BUT NEVER USED | 1 | Automated | Pending Fix |
| I007 | Informational | NAME MAPPING PARAMETERS | 1 | Automated | Pending Fix |

| S. No. | Severity | Bug Type | Instances | Detection Method | Status |
|---|---|---|---|---|---|
| I008 | Informational | REVERT STATEMENTS WITHIN EXTERNAL AND PUBLIC FUNCTIONS CAN BE USED TO PERFORM DOS ATTACKS | 1 | Automated | *Pending Fix* |
| I009 | Informational | USE SCIENTIFIC NOTATION | 1 | Automated | *Pending Fix* |
| G001 | Gas | ARRAY LENGTH CACHING | 1 | Automated | *Pending Fix* |
| G002 | Gas | AVOID RE-STORING VALUES | 2 | Automated | *Pending Fix* |
| G003 | Gas | AVOID ZERO-TO-ONE STORAGE WRITES | 1 | Automated | *Pending Fix* |
| G004 | Gas | CHEAPER INEQUALITIES IN IF() | 1 | Automated | *Pending Fix* |
| G005 | Gas | CHEAPER INEQUALITIES IN REQUIRE() | 2 | Automated | *Pending Fix* |
| G006 | Gas | DEFAULT INT VALUES ARE MANUALLY RESET | 3 | Automated | *Pending Fix* |
| G007 | Gas | DEFINE CONSTRUCTOR AS PAYABLE | 1 | Automated | *Pending Fix* |
| G008 | Gas | FUNCTIONS CAN BE IN-LINED | 7 | Automated | *Pending Fix* |
| G009 | Gas | REVERTING FUNCTIONS CAN BE PAYABLE | 5 | Automated | *Pending Fix* |
| G010 | Gas | GAS OPTIMIZATION IN INCREMENTS | 1 | Automated | *Pending Fix* |
| G011 | Gas | INTERNAL FUNCTIONS NEVER USED | 3 | Automated | *Pending Fix* |
| G012 | Gas | OPTIMIZING ADDRESS ID MAPPING | 2 | Automated | *Pending Fix* |
| G013 | Gas | STORAGE VARIABLE CACHING IN MEMORY | 4 | Automated | *Pending Fix* |
| G014 | Gas | UNNECESSARY CHECKED ARITHMETIC IN LOOP | 1 | Automated | *Pending Fix* |

# 05. Vulnerability Details

Issue Type

**APPROVE FRONT-RUNNING ATTACK**

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| H001 | High | Automated | 3 |

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_45 | -- | -- | *Pending Fix* |
| SSB_4236989_46 | -- | -- | *Pending Fix* |
| SSB_4236989_47 | -- | -- | *Pending Fix* |

**Upgrade your Plan to view the full report**

**3 High Issues Found**

Please upgrade your plan to view all the issues in your report.

Upgrade

Issue Type

**MODIFIER SIDE EFFECTS**

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| M001 | Medium | Automated | 1 |

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_4 | -- | -- | *Pending Fix* |

Issue Type

## USE OF FLOATING PRAGMA

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| L001 | Low | Automated | 10 |

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_18 | -- | -- | *Pending Fix* |
| SSB_4236989_19 | -- | -- | *Pending Fix* |
| SSB_4236989_19 | -- | -- | *Pending Fix* |
| SSB_4236989_19 | -- | -- | *Pending Fix* |
| SSB_4236989_19 | -- | -- | *Pending Fix* |

**Upgrade your Plan to view the full report**

**10 Low Issues Found**

Please upgrade your plan to view all the issues in your report.

Upgrade

Issue Type

**BLOCK VALUES AS A PROXY FOR TIME**

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| I001 | Informational | Automated | 2 |

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_57 | -- | -- | *Pending Fix* |
| SSB_4236989_58 | -- | -- | *Pending Fix* |

Issue Type

**ARRAY LENGTH CACHING**

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G001 | Gas | Automated | 1 |

### Description

During each iteration of the loop, reading the length of the array uses more gas than is necessary. In the most favora ble scenario, in which the length is read from a memory variable, storing the array length in the stack can save about 3 gas per iteration. In the least favorable scenario, in which external calls are made during each iteration, the amount of gas wasted can be significant.

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_32 | contract.sol | L963 - L967 | *Pending Fix* |

Issue Type

**AVOID RE-STORING VALUES**

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G002 | Gas | Automated | 2 |

### Description

The function is found to be allowing re-storing the value in the contract's state variable even when the old value is eq ual to the new value. This practice results in unnecessary gas consumption due to the `Gsreset` operation (2900 ga s), which could be avoided. If the old value and the new value are the same, not updating the storage would avoid thi s cost and could instead incur a `Gcoldsload` (2100 gas) or a `Gwarmaccess` (100 gas), potentially saving gas.

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_22 | contract.sol | L587 - L598 | *Pending Fix* |
| SSB_4236989_23 | contract.sol | L716 - L720 | *Pending Fix* |

Issue Type

## AVOID ZERO-TO-ONE STORAGE WRITES

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G003 | Gas | Automated | 1 |

### Description

Writing a storage variable from zero to a non-zero value costs 22,100 gas (20,000 for the write and 2,100 for cold access), making it one of the most expensive operations. This is why patterns like OpenZeppelin's `ReentrancyGuard` use `1` and `2` instead of `0` and `1`—to avoid the high cost of zero-to-non-zero writes. Non-zero to non-zero updates cost only 5,000 gas.

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_3 | contract.sol | L933 - L933 | *Pending Fix* |

Issue Type

## CHEAPER INEQUALITIES IN IF()

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G004 | Gas | Automated | 1 |

### Description

The contract was found to be doing comparisons using inequalities inside the if statement.
When inside the `if` statements, non-strict inequalities `(>=, <=)` are usually cheaper than the strict equalities `(>, <)`.

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_59 | contract.sol | L610 - L610 | *Pending Fix* |

Issue Type

## CHEAPER INEQUALITIES IN REQUIRE()

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G005 | Gas | Automated | 2 |

### Description

The contract was found to be performing comparisons using inequalities inside the `require` statement. When inside the `require` statements, non-strict inequalities `(>=, <=)` are usually costlier than strict equalities `(>, <)`.

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_60 | contract.sol | L941 - L941 | *Pending Fix* |
| SSB_4236989_61 | contract.sol | L961 - L961 | *Pending Fix* |

Issue Type

## DEFAULT INT VALUES ARE MANUALLY RESET

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G006 | Gas | Automated | 3 |

### Description

The contract is found to inefficiently reset integer variables to their default value of zero using manual assignment. In Solidity, manually setting a variable to its default value does not free up storage space, leading to unnecessary gas c onsumption. Instead, using the `.delete` keyword can achieve the same result while also freeing up storage space on the Ethereum blockchain, resulting in gas cost savings.

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_29 | contract.sol | L757 - L757 | *Pending Fix* |
| SSB_4236989_30 | contract.sol | L825 - L825 | *Pending Fix* |
| SSB_4236989_31 | contract.sol | L985 - L985 | *Pending Fix* |

Issue Type

## DEFINE CONSTRUCTOR AS PAYABLE

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G007 | Gas | Automated | 1 |

### Description

Developers can save around 10 opcodes and some gas if the constructors are defined as payable.
However, it should be noted that it comes with risks because payable constructors can accept ETH during deployme
nt.

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_5 | contract.sol | L932 - L935 | *Pending Fix* |

Issue Type

## FUNCTIONS CAN BE IN-LINED

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G008 | Gas | Automated | 7 |

### Description

The internal function was called only once throughout the contract. Internal functions cost more gas due to additiona l JUMP instructions and stack operations.

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_38 | contract.sol | L543 - L548 | *Pending Fix* |
| SSB_4236989_39 | contract.sol | L608 - L618 | *Pending Fix* |
| SSB_4236989_40 | contract.sol | L684 - L688 | *Pending Fix* |
| SSB_4236989_41 | contract.sol | L794 - L796 | *Pending Fix* |
| SSB_4236989_42 | contract.sol | L801 - L803 | *Pending Fix* |
| SSB_4236989_43 | contract.sol | L812 - L815 | *Pending Fix* |
| SSB_4236989_44 | contract.sol | L824 - L827 | *Pending Fix* |

Issue Type

## REVERTING FUNCTIONS CAN BE PAYABLE

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G009 | Gas | Automated | 5 |

### Description

If a function modifier such as `onlyOwner` is used, the function will revert if a normal user tries to pay the function. Marking the function as payable will lower the gas cost for legitimate callers because the compiler will not include checks for whether a payment was provided.

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_52 | contract.sol | L940 - L943 | *Pending Fix* |
| SSB_4236989_53 | contract.sol | L955 - L968 | *Pending Fix* |
| SSB_4236989_54 | contract.sol | L971 - L973 | *Pending Fix* |
| SSB_4236989_55 | contract.sol | L976 - L978 | *Pending Fix* |
| SSB_4236989_56 | contract.sol | L983 - L992 | *Pending Fix* |

Issue Type

## GAS OPTIMIZATION IN INCREMENTS

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G010 | Gas | Automated | 1 |

### Description

`++i` costs less gas compared to `i++` or `i += 1` for unsigned integers. In `i++`, the compiler has to create a temporary variable to store the initial value. This is not the case with `++i` in which the value is directly incremented and returne d, thus, making it a cheaper alternative.

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_49 | contract.sol | L963 - L963 | *Pending Fix* |

Issue Type

## INTERNAL FUNCTIONS NEVER USED

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G011 | Gas | Automated | 3 |

### Description

The contract declared internal functions but was not using them in any of the functions or contracts.
Since internal functions can only be called from inside the contracts, it makes no sense to have them if they are not u
sed. This uses up gas and causes issues for auditors when understanding the contract logic.

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_6 | contract.sol | L139 - L141 | *Pending Fix* |
| SSB_4236989_7 | contract.sol | L135 - L137 | *Pending Fix* |
| SSB_4236989_8 | contract.sol | L905 - L907 | *Pending Fix* |

Issue Type

## OPTIMIZING ADDRESS ID MAPPING

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G012 | Gas | Automated | 2 |

### Description

Combining multiple address/ID mappings into a single mapping using a struct enhances storage efficiency, simplifies code, and reduces gas costs, resulting in a more streamlined and cost-effective smart contract design.
It saves storage slot for the mapping and depending on the circumstances and sizes of types, it can avoid a Gsset (2 0000 gas) per mapping combined. Reads and subsequent writes can also be cheaper when a function requires both values and they fit in the same storage slot.

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_1 | contract.sol | L338 - L338 | *Pending Fix* |
| SSB_4236989_2 | contract.sol | L340 - L340 | *Pending Fix* |

Issue Type

## STORAGE VARIABLE CACHING IN MEMORY

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G013 | Gas | Automated | 4 |

### Description

The contract is using the state variable multiple times in the function.
SLOADs are expensive (100 gas after the 1st one) compared to MLOAD / MSTORE (3 gas each).

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_10 | contract.sol | L490 - L518 | *Pending Fix* |
| SSB_4236989_10 | contract.sol | L490 - L518 | *Pending Fix* |
| SSB_4236989_11 | contract.sol | L887 - L893 | *Pending Fix* |
| SSB_4236989_12 | contract.sol | L983 - L992 | *Pending Fix* |

Issue Type

## UNNECESSARY CHECKED ARITHMETIC IN LOOP

| S. No. | Severity | Detection Method | Instances |
|---|---|---|---|
| G014 | Gas | Automated | 1 |

### Description

Increments inside a loop could never overflow due to the fact that the transaction will run out of gas before the varia ble reaches its limits. Therefore, it makes no sense to have checked arithmetic in such a place.

| Bug ID | File Location | Line No. | Action Taken |
|---|---|---|---|
| SSB_4236989_33 | contract.sol | L963 - L963 | *Pending Fix* |

# 06. Scan History

Critical High Medium Low Informational Gas

| No | Date | Security Score | Scan Overview |
|---|---|---|---|
| 1. | 2025-07-22 | 89.80 | 0 4 1 12 14 33 |

# 07. Disclaimer

The Reports neither endorse nor condemn any specific project or team, nor do they guarantee the security of any specific project. The contents of this report do not, and should not be interpreted as having any bearing on, the economics of tokens, token sales, or any other goods, services, or assets.

The security audit is not meant to replace functional testing done before a software release.

There is no warranty that all possible security issues of a particular smart contract(s) will be found by the tool, i.e., It is not guaranteed that there will not be any further findings based solely on the results of this evaluation.

Emerging technologies such as Smart Contracts and Solidity carry a high level of technical risk and uncertainty. There is no warranty or representation made by this report to any Third Party in regards to the quality of code, the business model or the proprietors of any such business model, or the legal compliance of any business.

In no way should a third party use these reports to make any decisions about buying or selling a token, product, service, or any other asset. It should be noted that this report is not investment advice, is not intended to be relied on as investment advice, and has no endorsement of this project or team. It does not serve as a guarantee as to the project's absolute security.

The assessment provided by SolidityScan is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. SolidityScan owes no duty to any third party by virtue of publishing these Reports.

As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent manual audits including manual audit and a public bug bounty program to ensure the security of the smart contracts.