StakingRewardsCalculator Contract

Reown (fka WalletConnect)

HALBORN

StakingRewardsCalculator Contract - Reown (fka WalletConnect)

Prepared by: HALBORN

Last Updated Unknown date

Date of Engagement: January 29th, 2025 - January 30th, 2025

Summary

100% OF ALL REPORTED FINDINGS HAVE BEEN ADDRESSED

ALL FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
2	0	0	0	0	2

TABLE OF CONTENTS

1. Introduction

`Wallet Connect Foundation` engaged `Halborn` to conduct a security assessment on their smart contracts beginning on January 29th, 2025 and ending on January 30th, 2025. The security assessment was scoped to the smart contracts provided to Halborn. Commit hashes and further details can be found in the Scope section of this report.

The `Wallet Connect Foundation` codebase in scope mainly consists of a smart contract that allow for calculating and injecting weekly staking rewards based on Thursday 00:00 UTC snapshots.

2. Assessment Summary

`Halborn` was provided 2 days for the engagement and assigned 1 full-time security engineer to review the security of the smart contracts in scope. The engineer is a blockchain and smart contract security expert with advanced penetration testing and smart contract hacking skills, and deep knowledge of multiple blockchain protocols.

The purpose of the assessment is to:

- Identify potential security issues within the smart contracts.
- Ensure that smart contract functionality operates as intended.

In summary, `Halborn` identified some improvements to reduce the likelihood and impact of risks, which were addressed by the `Wallet Connect Foundation team`. The main ones were the following:

- `Combine the divisors into a single division operation to minimize potential rounding errors.`
- `Emit events for all state changes.`

3. Test Approach And Methodology

`Halborn` performed a combination of manual review of the code and automated security testing to balance efficiency, timeliness, practicality, and accuracy in regard to the scope of this assessment. While manual testing is recommended to uncover flaws in logic, process, and implementation; automated testing techniques help enhance coverage of smart contracts and can quickly identify items that do not follow security best practices.

The following phases and associated tools were used throughout the term of the assessment:

- Research into architecture, purpose and use of the platform.
- Smart contract manual code review and walkthrough to identify any logic issue.
- Thorough assessment of safety and usage of critical Solidity variables and functions in scope that could led to arithmetic related vulnerabilities.
- Local testing with custom scripts (`Foundry`).
- Fork testing against main networks (`Foundry`).
- Static analysis of security for scoped contract, and imported functions (`Slither`).

4. Caveats

The current security assessment was limited to the following:

- The `StakingRewardsCalculator` contract was reviewed in its entirety.
- The `WalletConnectConfig` contract assessment was scoped to **changes made in PR** shared by the `Wallet Connect Foundation` team.

It's important to note that despite these caveats, the security assessment aimed to provide a thorough evaluation of the protocol's security posture. However, the limitations mentioned above should be considered when interpreting the findings and recommendations.

5. RISK METHODOLOGY

Every vulnerability and issue observed by Halborn is ranked based on **two sets** of **Metrics** and a **Severity Coefficient**. This system is inspired by the industry standard Common Vulnerability Scoring System.

The two **Metric sets** are: **Exploitability** and **Impact**. **Exploitability** captures the ease and technical means by which vulnerabilities can be exploited and **Impact** describes the consequences of a successful exploit.

The **Severity Coefficients** is designed to further refine the accuracy of the ranking with two factors: **Reversibility** and **Scope**. These capture the impact of the vulnerability on the environment as well as the number of users and smart contracts affected.

The final score is a value between 0-10 rounded up to 1 decimal place and 10 corresponding to the highest security risk. This provides an objective and accurate rating of the severity of security vulnerabilities in smart contracts.

The system is designed to assist in identifying and prioritizing vulnerabilities based on their level of risk to address the most critical issues in a timely manner.

5.1 EXPLOITABILITY

ATTACK ORIGIN (AO):

Captures whether the attack requires compromising a specific account.

ATTACK COST (AC):

Captures the cost of exploiting the vulnerability incurred by the attacker relative to sending a single transaction on the relevant blockchain. Includes but is not limited to financial and computational cost.

ATTACK COMPLEXITY (AX):

Describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability. Includes but is not limited to macro situation, available third-party liquidity and regulatory challenges.

METRICS:

EXPLOITABILITY METRIC (M_E)	METRIC VALUE	NUMERICAL VALUE
Attack Origin (AO)	Arbitrary (AO:A) Specific (AO:S)	1 0.2
Attack Cost (AC)	Low (AC:L) Medium (AC:M) High (AC:H)	1 0.67 0.33
Attack Complexity (AX)	Low (AX:L) Medium (AX:M) High (AX:H)	1 0.67 0.33

Exploitability E is calculated using the following formula:

$$E = \prod m_e$$

5.2 IMPACT

CONFIDENTIALITY (C):

Measures the impact to the confidentiality of the information resources managed by the contract due to a successfully exploited vulnerability. Confidentiality refers to limiting access to authorized users only.

INTEGRITY (I):

Measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of data stored and/or processed on-chain. Integrity impact directly affecting Deposit or Yield records is excluded.

AVAILABILITY (A):

Measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability. This metric refers to smart contract features and functionality, not state. Availability impact directly affecting Deposit or Yield is excluded.

DEPOSIT (D):

Measures the impact to the deposits made to the contract by either users or owners.

YIELD (Y):

Measures the impact to the yield generated by the contract for either users or owners.

METRICS:

IMPACT METRIC (M_I)	METRIC VALUE	NUMERICAL VALUE
Confidentiality (C)	None (C:N) Low (C:L) Medium (C:M) High (C:H) Critical (C:C)	0 0.25 0.5 0.75 1
Integrity (I)	None (I:N) Low (I:L) Medium (I:M) High (I:H) Critical (I:C)	0 0.25 0.5 0.75 1
Availability (A)	None (A:N) Low (A:L) Medium (A:M) High (A:H) Critical (A:C)	0 0.25 0.5 0.75 1
Deposit (D)	None (D:N) Low (D:L) Medium (D:M) High (D:H) Critical (D:C)	0 0.25 0.5 0.75 1
Yield (Y)	None (Y:N) Low (Y:L) Medium (Y:M) High (Y:H) Critical (Y:C)	0 0.25 0.5 0.75 1

Impact I is calculated using the following formula:

$$I = max(m_I) + \frac{\sum m_I - max(m_I)}{4}$$

5.3 SEVERITY COEFFICIENT

REVERSIBILITY (R):

Describes the share of the exploited vulnerability effects that can be reversed. For upgradeable contracts, assume the contract private key is available.

SCOPE (S):

Captures whether a vulnerability in one vulnerable contract impacts resources in other contracts.

METRICS:

SEVERITY COEFFICIENT (C)	COEFFICIENT VALUE	NUMERICAL VALUE
Reversibility (r)	None (R:N) Partial (R:P) Full (R:F)	1 0.5 0.25
Scope (s)	Changed (S:C) Unchanged (S:U)	1.25 1

Severity Coefficient C is obtained by the following product:

$$C = rs$$

The Vulnerability Severity Score S is obtained by:

$$S = min(10, EIC * 10)$$

The score is rounded up to 1 decimal places.

SEVERITY	SCORE VALUE RANGE
Critical	9 - 10
High	7 - 8.9

SEVERITY	SCORE VALUE RANGE
Medium	4.5 - 6.9
Low	2 - 4.4
Informational	0 - 1.9

6. SCOPE

REPOSITORY

(a) Repository: contracts

(b) Assessed Commit ID: 4651755

(c) Items in scope:

- src/WalletConnectConfig.sol
- src/StakingRewardsCalculator.sol

Out-of-Scope: Third party dependencies and economic attacks.

Out-of-Scope: New features/implementations after the remediation commit IDs.

7. ASSESSMENT SUMMARY & FINDINGS OVERVIEW

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
0	0	0	0	2

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION DATE
SUBOPTIMAL DIVISION ORDER IN WEEKLY REWARDS CALCULATION	INFORMATIONAL	SOLVED - 02/02/2025
MISSING EVENT	INFORMATIONAL	SOLVED - 02/02/2025

8. FINDINGS & TECH DETAILS

8.1 SUBOPTIMAL DIVISION ORDER IN WEEKLY REWARDS CALCULATION

// INFORMATIONAL

Description

In the `calculateWeeklyRewards()` function, the weekly rewards calculation performs sequential divisions which could lead to unnecessary precision loss. The current implementation divides `annualRewardsWithPrecision` first by `WEEKS_IN_YEAR` and then by `(PRECISION * 100)`:

```
208 | weeklyRewards = (annualRewardsWithPrecision / WEEKS_IN_YEAR) / (PRECISION * 100);
```

While mathematically equivalent, performing divisions sequentially can lead to more rounding errors in Solidity due to integer division truncation at each step. Each division operation potentially truncates the result, and when performed sequentially, these truncations compound.

BVSS

AO:S/AC:L/AX:L/R:N/S:U/C:N/A:N/I:L/D:N/Y:N (0.5)

Recommendation

Combine the divisors into a single division operation to minimize potential rounding errors:

```
weeklyRewards = annualRewardsWithPrecision / (PRECISION * 100 * WEEKS_IN_YEAR);
```

Remediation Comment

SOLVED: The **Wallet Connect Foundation team** solved this finding in commit `fedc68a` by following the mentioned recommendation.

References

WalletConnectFoundation/contracts/src/StakingRewardsCalculator.sol#L208

8.2 MISSING EVENT

// INFORMATIONAL

Description

The `injectRewardsForWeek()` function in the `StakingRewardsCalculator` contract does not emit an event. In Solidity development, emitting events is a recommended practice when state-changing functions are invoked. This absence may hamper effective state tracking in off-chain monitoring systems.

BVSS

AO:A/AC:L/AX:L/R:N/S:U/C:N/A:N/I:N/D:N/Y:N (0.0)

Recommendation

Emit events for all state changes that occur as a result of administrative functions to facilitate off-chain monitoring of the system.

Remediation Comment

SOLVED: The **Wallet Connect Foundation team** solved this finding in commit `d8679b9` by following the mentioned recommendation.

References

WalletConnectFoundation/contracts/src/StakingRewardsCalculator.sol#L94-L137

9. AUTOMATED TESTING

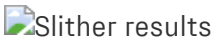
STATIC ANALYSIS REPORT

Description

`Halborn` used automated testing techniques to enhance the coverage of certain areas of the smart contracts in scope. Among the tools used was Slither, a Solidity static analysis framework. After `Halborn` verified the smart contracts in the repository and was able to compile them correctly into their abis and binary format, Slither was run against the contracts. This tool can statically verify mathematical relationships between Solidity variables to detect invalid or inconsistent usage of the contracts' APIs across the entire code-base.
The security team assessed all findings identified by the Slither software, however, findings with related to external dependencies are not included in the below results for the sake of report readability.

Output

The findings obtained as a result of the Slither scan were reviewed, and were not included in the report because they were determined as false positives.


Slither results

---

addressing potential vulnerabilities introduced by code modifications.