expelee

Building the Futuristic Blockchain Ecosystem

SECURITY AUDIT REPORT

Cremation Stake

TABLE OF CONTENTS

OVERVIEW

The Cremation Stake contract is designed to facilitate staking and reward distribution for a specific token. Users can stake tokens for different staking periods (short, medium, long) and receive rewards based on the staking period.

Contracts

Reviewied contract
Test

Report Date : 03.09.2023

Scope and Summary
The following smart contracts were in scope of the audit:
• *cremation_stake*
The following number of issues were found, categorized by their severity:

OVERVIEW

Risk Findings

Severity	Found	Pending	Resolved
● High	0	0	0
● Medium	0	0	0
● Low	0	2	0
● Informational	0	0	0
● **Total**	**0**	**2**	**0**

RISK CLASSIFICATION

Risk Classification

High

Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, of the contract and its functions. Must be fixed as soon as possible.

Medium

Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Must be fxed as soon as possible.

Low

Effects are minimal in isolation and do not pose a signifcant danger to the project or its users. Issues under this classifcation are recommended to be fixed nonetheless.

Informational

A vulnerability that have informational character but is not effecting any of the code

RISK FINDING

[L-01] Lack of Validation for Staking Amount

Severity : Low

Description

· The receive_cw20 function allows users to stake tokens. However, there is no validation to check if the staking amount is greater than 0.

Mitigation

```
if amount.is_zero() { return
Err(ContractError::InvalidStakeAmount {}); }
```

· Implement input validation at the beginning of the receive_cw20 function to ensure that the staking amount is greater than 0.

· Reject transactions with an appropriate error message if the staking amount is 0.

RISK FINDING

[L-02] Insufficient Balance Check

Severity : Low

Description

· Please check sufficient balance of tokens to stake if there is a exact amount of token to stake.

Mitigation

```
let user_balance = query_token_balance(deps.as_ref(),
&sender)?; if user_balance < amount { return
Err(ContractError::InsufficientBalance {}); } 2
```

· Ensure that the user has a balance greater than or equal to the staking amount. · Reject transactions with an appropriate error message if the user's balance is insufficient for staking.

ABOUT EXPELEE

Expelee is a product-based aspirational Web3 start-up. Coping up with numerous solutions for blockchain security and constructing a Web3 ecosystem from deal making platform to developer hosting open platform, while also developing our own commercial and sustainable blockchain.

🌐 www.expelee.com

🐦 expeleeofficial   Ⓜ expelee

✈ Expelee   in expelee

📷 expelee_official   💻 expelee-co

exp̂elee

Building the Futuristic Blockchain Ecosystem

DISCLAIMER

This audit report is prepared for informational purposes only and does not constitute financial, legal, or professional advice. The audit has been conducted based on the information provided by the project team and is limited to the code and documentation available up to the audit date. The assessment is focused on identifying potential vulnerabilities and security concerns within the provided codebase. It does not guarantee the absence of vulnerabilities or the security of the system. The audit does not include a comprehensive review of the project's business model, economic viability, or other non-technical aspects. The audit report is not an endorsement of the project, and readers should exercise their own judgment and due diligence before using, investing, or participating in the project. The project team and the auditors are not liable for any losses, damages, or expenses that may arise from actions taken based on this audit report. The audit is based on the current state of the code and may not account for future changes, updates, or modifications. Security is an ongoing process, and the project team is responsible for addressing any identified issues and maintaining the security of the system beyond the scope of this audit. Readers are encouraged to consult with their own professional advisors for advice tailored to their individual circumstances before making any decisions related to the project. This audit report is provided on an "as is' basis and without any warranties, representations, or guarantees.

expelee

Building the Futuristic Blockchain Ecosystem