FECHA: 29/08/2023

Smart Contract Audit Report – BNB AllStars

Summary

This report presents the results of the audit conducted on the provided smart contract. The contract implements an investment and reward system based on cryptocurrencies. The aim of the audit was to identify potential vulnerabilities, security risks, and areas for improvement in the code.

TestNet:

https://testnet.bscscan.com/address/0x964C71Be189bc93A75aCF05179B5899558C58DC6

Executive Summary

During the audit, a thorough examination of the contract's functions and features was conducted to assess its security and compliance with best practices in Solidity development. The review included evaluating 50 possible known vulnerabilities as well as inspecting the provided code to identify risks and areas for improvement. Key findings and recommendations based on the analysis are presented below.

CHAINAUDIT

FECHA: 29/08/2023

Important Contract Details

Chain: BSC

Token: BNB

DApp Type: ROI DAPP

Daily ROI Percentage: 1.5%

Minimum Investment: 0.1 BNB

Maximum Investment: 25 BNB

Maximum Withdrawal: 200 BNB

Minimum Airdrop: 0.1 BNB

Accumulation Rewards Limit: 200 BNB

Mandatory Reinvestment: 3 times (Static - Irreversible)

Reinvestment Bonus: 1%

CHAINAUDIT

FECHA: 29/08/2023

Critical Vulnerability Findings

After conducting a comprehensive analysis of the smart contract using over 50 hacks and potential vulnerabilities, the following critical findings have been identified:

1. **Reentrancy:** Not vulnerable. The contract uses the 'notReentrant' modifier to prevent reentrancy attacks.

2. **Integer Overflow and Underflow:** Not vulnerable. The use of the SafeMath library prevents overflow and underflow issues.

3. **Delegatecall to Untrusted Callee:** Not vulnerable. Untrusted delegates to addresses are not used.

4. **Timestamp Dependence:** Not vulnerable. The contract does not rely on the value of 'block.timestamp'.

5. **State Variable Manipulation:** Not vulnerable. Critical state variables are adequately protected.

CHAINAUDIT

FECHA: 29/08/2023

Findings and Recommendations

The following are the key findings identified during the audit, along with corresponding recommendations:

1. **Overflow and Underflow Handling:**
   - ❖ The contract implements measures to prevent overflow and underflow in critical mathematical operations, which mitigates risks associated with these issues.

2. **Input Validation:**
   - ❖ The code includes validations to prevent invalid user inputs, which is essential to ensure the integrity of the system.

3. **Referral System Security:**
   - ❖ The implementation of the referral system appears robust and does not present evident abuse risks.

4. **Administrative Functions:**
   - ❖ The contract includes administrative functions that allow the owner to change contract properties and features. These functions should be used with caution and transparency.

5. **Data Privacy:**
   - ❖ It is recommended to assess the exposure of sensitive user data such as usernames and statistics. Measures can be implemented to enhance user privacy

FECHA: 29/08/2023

Owner Privileges

The smart contract includes a set of functions that grant exclusive privileges to the contract owner. These functions enable the owner to perform critical actions that can affect the operation of the contract and its users. Below are the functions and their respective actions:

1. CHANGE_OWNERSHIP
   - Description: Changes the address of the contract owner.
   - Action: Allows the owner to transfer contract ownership to a specific address.
   - Restriction: Can only be executed by the current contract owner

2. CHANGE_PROJECT_WALLET
   - Description: Changes the project wallet address.
   - Action: Enables the owner to change the address to which project funds are sent.
   - Restriction: Can only be executed by the current contract owner.

3. ENABLE_AIRDROP
   - Description: Enables the airdrop functionality.
   - Action: Allows the owner to activate the ability to perform airdrops in the contract (irreversible).
   - Restriction: Can only be executed by the current contract owner.

4. SET_STARTED
    - ❖ Description: Sets the contract's start status.
    - ❖ Action: Allows the owner to define whether the contract has started or not.
    - ❖ Restriction: Can only be executed by the current contract owner.

These functions provide the contract owner with a significant level of control over its operation and features. It's important for the owner to use these functions with care and responsibility, as their actions can directly impact users and the overall functioning of the contract. The contract client is advised to be aware of these functions and their implications before deploying the contract in a production environment.

FECHA: 29/08/2023

Conclusions

Based on the review of the smart contract, it is concluded that it presents a solid and secure implementation. No significant vulnerabilities that could be exploited through the analyzed attack vectors were identified. However, it is recommended to continue practicing a rigorous security approach and conducting thorough testing to ensure the integrity of the system under real-world usage conditions.

Rating

The rating assigned to this smart contract is **9** on a scale of 0 to 10. This rating reflects a robust implementation with proper security practices. Further audits are encouraged in case of future modifications to ensure the security and operation of the system

This audit report is based on the analysis of the provided smart contract and implemented security practices

CHAINAUDIT

FRANCIS K.

AUDITOR FOR CHAINAUDIT

BNB All - Stars

CHAINAUDIT

FECHA: 29/08/2023