RIF On Chain

SECURITY ASSESSMENT REPORT

June 2023

Executive Summary

In June 2023, the IOVLabs Security team was engaged to perform a review on the proposal for Enhancing Transaction Cost Management for Users with Ethereum-based Gas Price Setting. The assessment analyzed the solution's codebase, architecture, and attack resilience. The objective was to identify potential vulnerabilities and evaluate the effectiveness of the proposed solution.

The assessment revealed that the proposed solution does not add any vulnerabilities and does not negatively affect the protocol.

Project Dashboard

Application Summary

Name	RIF on Chain
Assets	https://github.com/money-on-chain/RDOC-Contract https://github.com/money-on-chain/price-feeder https://github.com/money-on-chain/moc_prices_source https://github.com/money-on-chain/main-RBTC-contract
Version	https://github.com/money-on-chain/main-RBTC-contract/pull/114 https://github.com/money-on-chain/RDOC-Contract/pull/52
Language	Solidity

Proposal Description

As stated in the money on chain forum, the proposal for enhancing transaction cost management introduces a modifier in each operation that validates the `gas price` and rejects the transactions if it exceeds the threshold. By incorporating this modifier, we can effectively prevent transactions with excessive gas prices from being processed.

To ensure comprehensive coverage, it is necessary to apply this modifier for the `redeem` and `mint` operations over every token in the protocol.

The proposal also indicates that in order to maintain the integrity and usability of the protocol, it is crucial to allow modification of the gas price threshold through an address with the same authority as to pause the protocol. This restriction will ensure that any changes made to the threshold are carried out through authorization via governance.

Assuming that users will operate with the `gas price` reported by the RSK network node to set the initial threshold, the suggestion is to take the historical maximum of the last year plus 1 wei. That gives a value of `0.0658 Gwei`.

Assessment Results

During the assessment, our thorough analysis revealed that the proposed changes did not introduce any vulnerabilities to the protocol. The implemented modifications align perfectly with the proposal, ensuring a seamless integration and compatibility.

Furthermore, we conducted a comprehensive verification process and confirmed that the gas price threshold can only be modified by authorized entities. Specifically, only the address with the designated authority to pause the protocol through governance authorization has the capability to make such adjustments. This stringent control mechanism provides an additional layer of security, minimizing the risk of unauthorized manipulation of gas prices.

Overall, our assessment affirms that the proposed changes have been successfully implemented without compromising the system's security. The adherence to the proposal and the strict authorization requirements for modifying the gas price threshold contribute to a robust and secure protocol framework.

Disclaimer

This report is based on information provided to us and our own observations during the audit as stated above. We have conducted the audit in accordance with generally accepted cybersecurity auditing standards. However, our audit has limitations, and we cannot guarantee that all vulnerabilities and security issues have been identified. This report is provided for informational purposes only and should not be relied upon as a complete representation of the security of the protocol's information systems. We do not accept responsibility for any losses or damages that may arise from the use of this report or any reliance on the findings contained herein. It is important to note that cybersecurity threats are constantly evolving, and the protocol's security posture may change at any time. Our findings are accurate as of the date of the audit and may not reflect the current state of the protocol's security posture. This assessment should not be used in any way to make decisions around investment or involvement with any particular project. This assessment in no way provides investment advice, nor should be leveraged as investment advice of any sort.