VERILOG

2023

MANTLE MDI QUESTS:

SECURITY REVIEW REPORT

Sep 28, 2023

Contents

1 | Introduction

Figure 1.1: Mantle MDI Quests Report Cover

This report presents our engineering engagement with the Mantle team on the development of their dynamic NFT - Mantle MDI Quests.

Project Name	**Mantle MDI Quests**
Repository Link	https://github.com/mantle-xyz/mdi-quests
First Commit Hash	First: 8d24fc3;
Final Commit Hash	Final: 91ed139;
Language	Solidity
Chain	Mantle

2 | About Verilog Solutions

Founded by a group of cryptography researchers and smart contract engineers in North America, Verilog Solutions elevates the security standards for Web3 ecosystems by being a full-stack Web3 security firm covering smart contract security, consensus security, and operational security for Web3 projects.

Verilog Solutions team works closely with major ecosystems and Web3 projects and applies a quality above quantity approach with a continuous security model. Verilog Solutions onboards the best and most innovative projects and provides the best-in-class advisory services on security needs, including on-chain and off-chain components.

3 | Service Scope

3.1 | Service Stages

Our auditing service includes the following two stages:

- Smart Contract Auditing Service

3.1.1 | Smart Contract Auditing Service

The Verilog Solutions team analyzed the entire project using a detailed-oriented approach to capture the fundamental logic and suggested improvements to the existing code. Details can be found under Findings And Improvement Suggestions.

3.2 | Methodology

- **Code Assessment**
  - □ We evaluate the overall quality of the code and comments as well as the architecture of the repository.
  - □ We help the project dev team improve the overall quality of the repository by providing suggestions on refactorization to follow the best practices of Web3 software engineering.
- **Code Logic Analysis**
  - □ We dive into the data structures and algorithms in the repository and provide suggestions to improve the data structures and algorithms for the lower time and space complexities.
  - □ We analyze the hierarchy among multiple modules and the relations among the source code files in the repository and provide suggestions to improve the code architecture with better readability, reusability, and extensibility.
- **Business Logic Analysis**
  - □ We study the technical whitepaper and other documents of the project and compare its specifications with the functionality implemented in the code for any potential mismatch between them.
  - □ We analyze the risks and potential vulnerabilities in the business logic and make suggestions to improve the robustness of the project.
- **Access Control Analysis**
  - □ We perform a comprehensive assessment of the special roles of the project, including their authorities and privileges.
  - □ We provide suggestions regarding the best practice of privilege role management according to the standard operating procedures (SOP).
- **Off-Chain Components Analysis**
  - □ We analyze the off-chain modules that are interacting with the on-chain functionalities and provide suggestions according to the SOP.
  - □ We conduct a comprehensive investigation for potential risks and hacks that may happen on the off-chain components and provide suggestions for patches.

3.3 | Audit Scope

Our auditing for Mantle L2 Dynamic NFT - Mantle MDI Quests covered the Solidity smart contracts under the folder 'contracts' in the repository (https://github.com/mantle-xyz/mdi-quests) with commit hash **8d24fc3**.

4 | Findings and Improvement Suggestions

Severity	Total	Acknowledged	Resolved
High	0	0	0
Medium	0	0	0
Low	2	2	2
Informational	0	0	0

4.1 | Low

4.1.1 | Use `_safeMint()` instead of `_mint()`

Severity	Low

Source	mdi-quests-contract/src/MantleBase.sol#L82;
	mdi-quests-contract/src/MantleBase.sol#L93;

Commit	8d24fc3;
Status	Resolved in commit f969f30;

- **Description**
  The `_safeMint()` function can be used instead of `_mint()` to ensure that the NFT can only be minted to an EOA or contract implemented with IERC721Receiver-onERC721Received.

- **Exploit Scenario**
  N/A.

- **Recommendations**
  Please consider using `_safeMint()` instead of `_mint()`.

- **Results**
  Resolved in commit f969f30.

  The suggestion was implemented.

4.1.2 | Lack of event emission for critical operations

Severity	Low

Source	mdi-quests-contract/src/MantleBase.sol#L134;
	mdi-quests-contract/src/MantleBase.sol#L152;

Commit	8d24fc3;
Status	Resolved in commit f969f30;

- **Description**
  Events are vital aids in monitoring contracts and detecting suspicious behavior. The `setMerkleRoot()` and `setUriPrefix()` both perform important operations but don't emit events.

- **Exploit Scenario**
  N/A.

- **Recommendations**
  Create events for the functions mentioned above.

- **Results**
  Resolved in commit f969f30.

  The suggestion was implemented.

5 | Notes and Additional Information

5.1 | NFT Mint Flow

- There is a total supply of 100k **NFT**
  - Only 50k will be released based on **whitelist minting**
  - Batch mint function will be utilized to mint the remaining NFTs to the admin wallet for future reward distribution
  - Free mint with network fees in MNT
  - Each whitelisted wallet can only mint 1 NFT
- If the wallet is a whitelisted wallet, the user will be able to proceed with the minting
- If the wallet is not whitelisted, the user is not able to mint
- **Variable NFT image**: Given that the NFT collection is dynamic and upgradeable, it's been decided that NFT image tokenURI will be an S3 link instead of IPFS

6 | Appendix

6.1 | Appendix I: Severity Categories

Severity	Description
High	Issues that are highly exploitable security vulnerabilities. It may cause direct loss of funds / permanent freezing of funds. All high severity issues should be resolved.
Medium	Issues that are only exploitable under some conditions or with some privileged access to the system. Users' yields/rewards/information is at risk. All medium severity issues should be resolved unless there is a clear reason not to.
Low	Issues that are low risk. Not fixing those issues will not result in the failure of the system. A fix on low severity issues is recommended but subject to the clients' decisions.
Informationa	Issues that pose no risk to the system and are related to the security best practices. Not fixing those issues will not result in the failure of the system. A fix on informational issues or adoption of those security best practices-related suggestions is recommended but subject to clients' decision.

6.2 | Appendix II: Status Categories

Severity	Description
Unresolved	The issue is not acknowledged and not resolved.
Partially Resolved	The issue has been partially resolved
Acknowledged	The Finding / Suggestion is acknowledged but not fixed / not implemented.
Resolved	The issue has been sufficiently resolved

7 | Disclaimer

Verilog Solutions receives compensation from one or more clients for performing the smart contract and auditing analysis contained in these reports. The report created is solely for Clients and published with their consent. As such, the scope of our audit is limited to a review of code, and only the code we note as being within the scope of our audit is detailed in this report. It is important to note that the Solidity code itself presents unique and unquantifiable risks since the Solidity language itself remains under current development and is subject to unknown risks and flaws. Our sole goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies. Thus, Verilog Solutions in no way claims any guarantee of security or functionality of the technology we agree to analyze.

In addition, Verilog Solutions reports do not provide any indication of the technology's proprietors, business, business model, or legal compliance. As such, reports do not provide investment advice and should not be used to make decisions about investment or involvement with any particular project. Verilog Solutions has the right to distribute the Report through other means, including via Verilog Solutions publications and other distributions. Verilog Solutions makes the reports available to parties other than the Clients (i.e., "third parties") – on its website in hopes that it can help the blockchain ecosystem develop technical best practices in this rapidly evolving area of innovation.