SECURITY AUDIT OF

MILADY MEME COIN API BACKEND

Public Report

May 16, 2023

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

EXECUTIVE SUMMARY

During the audit process, the audit team had identified some vulnerable issues in the application, along with some recommendations. Milady Meme Coin API Backend has passed with no Low, Medium, High, or Critical severity issues. But audit team have some recommendations about system design, smart contract and sensitive data.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About Milady Meme Coin API Backend

The meme coin of Milady NFT collection. LADYS is the tokenisation of the fully memetically optimized white pill.LADYS is not another meme coin. LADYS is a self-organised meme coin. LADYS is the drip currency. LADYS is the points for karma, charm and beauty. LADYS is the accumulation of clout.Milady meme coin is LADYS, and LADYS is the meme coin for Milady.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the Milady Meme Coin API Backend.

Folder	SHA256 Sum
guard-api	c399f44f6ff99d5690aa29f9ddfbc220fd3e482b7f02c7b1562396be685b9252
subscribe-jobs	48098bf824ff1614e6fd82a485e24118b239c25e93f92f2dd5b4bccc0bdb58f7
bridge-api	60ecbad4a1cb5e6b6d12187b6a6b30430968ca041d1ad851a3e48369047235d3

Table 1. Audit scope

1.3. Audit methodology

Our security audit process includes three steps:

- Mechanism Design is reviewed to look for any potential problems.
- Source codes are scanned/tested for commonly known and more specific vulnerabilities using public and our in-house security analysis tool.
- Manual audit of the codes for security issues. The source code is manually analyzed to look for any potential problems.

For vulnerabilities, we categorize the findings into categories as listed in table below, depending on their severity level:

SEVERITY LEVEL	DESCRIPTION
CRITICAL	A vulnerability that can disrupt the contract functioning; creates a critical risk to the contract; required to be fixed immediately.
HIGH	A vulnerability that could affect the desired outcome of executing the contract with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the contract with medium impact in a specific scenario; needs to be fixed.
LOW	An issue that does not have a significant impact, can be considered as less important.

Table 2. Severity levels

1.4. Disclaimer

Please note that security auditing cannot uncover all existing vulnerabilities, and even an audit in which no vulnerabilities are found is not a guarantee for a 100% secure application. However, auditing allows discovering vulnerabilities that were unobserved, overlooked during development and areas where additional security measures are necessary.

2. AUDIT RESULT

2.1. Overview

The Milady Meme Coin API Backend consists of three interconnected modules, which are as blue highlight follows:

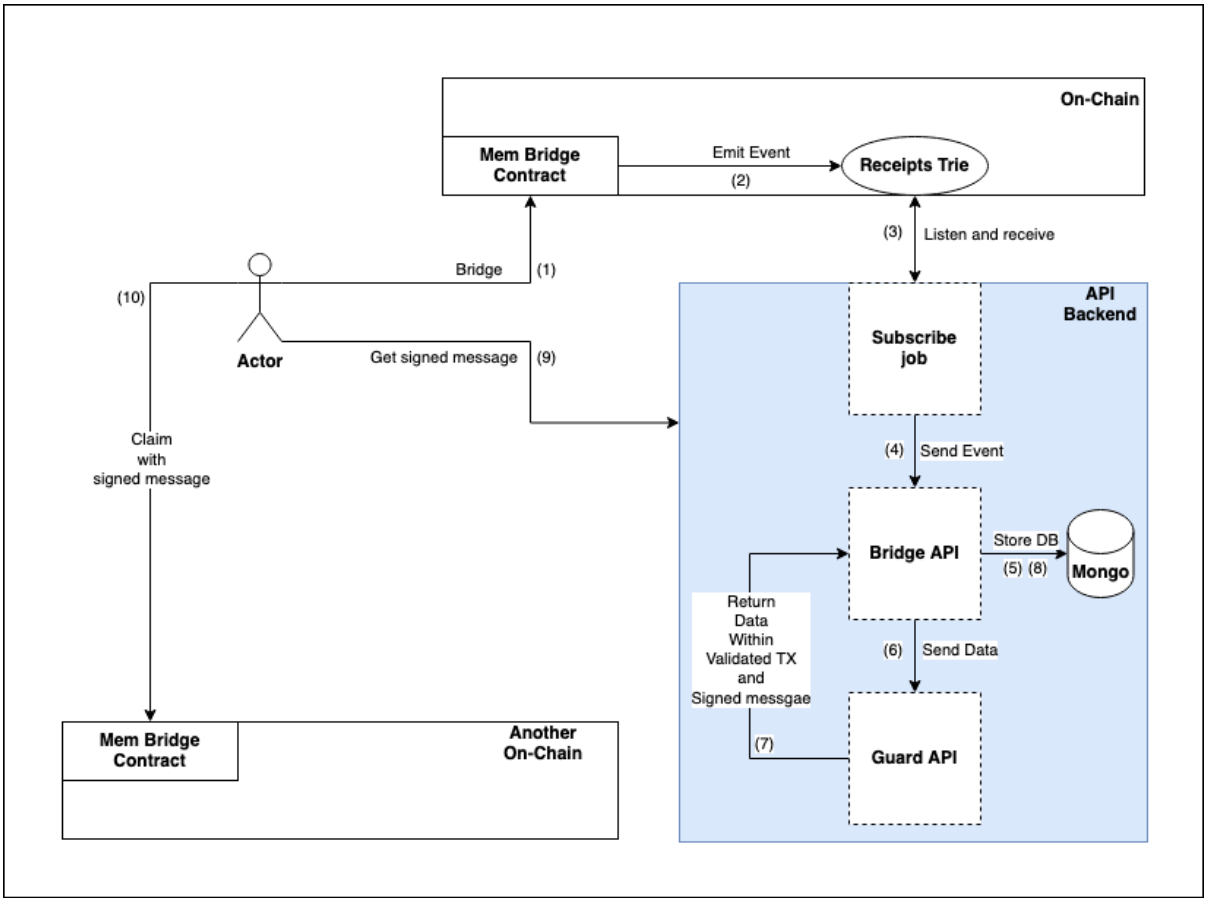

Image 1. Milady Meme Coin API Backend workflow

After a successful claim, the contract emits an event which is received by the Subscribe Job module. This module then sends a request to the Bridge API to update the claimed status in the database.

2.1.1. Subscribe job

The module is written in `Javascript` language. The process involves periodically listening to events emitted by on-chain contracts at a specified time interval and handling each event by sending it to the bridge API with a corresponding topic.

2.1.2. Bridge API

The module is written in `Python` language. It is designed to receive requests from a subscription job, process and update the `Mongo` database, and initiate calls to the guard API for the purpose of transaction verification, message signing, and recording the results in the database.

Besides, the module interact with database to update when TX has claimed.

2.1.3. Guard API

The module is written in `Python` language. Its purpose is transaction verification and message signing.

2.2. Architecture Security

This section provides a summary of the security assumptions of the architecture. These assumptions are considered trustworthy without requiring any verification or disputation. In addition, we analyze the current security controls and identify gaps in the security assumptions. Finally, we offer recommendations to improve the security of the architecture.

2.2.1. Security Controls and Gaps

The security assumptions only worked if the smart contracts were correctly implemented and proper out-of-chain security controls.

- **There is no risk of complete loss if the threshold of governance private keys are secured.**
    - We assume that all governance private keys should be protected by hardware wallets.
    - We assume that the threshold of governance voting should justify the risk of complete loss.
- **There is no risk of complete loss if the human private key is secured.**
    - We assume that the human private key should be protected in hardware wallets. While it is fairly low risk that all validators plus the private key are compromised; the role of the special person is not clearly defined
- **Censorship is unlikely.**
    - We assume that all governance private keys are available in case to vote out the malicious validators.

2.2.2. Security Recommendation

Below are our recommendations for a more secure architecture and design of Milady Meme Coin API Backend.

System Design

In order to ensure the security of the system, it is crucial to have a service in place that can detect any abnormal or suspicious activity related to the bridge or large token amounts. This service should be designed to monitor the system closely, and be capable of recognizing any anomalous activity that may indicate an attack or malicious intent. For example, the service should be able to identify and notify the relevant parties of any attempts to claim funds with a transaction that is not present in the database. By having such a service in place, the system can take proactive measures to prevent and mitigate any potential threats to the security of the network.

Smart Contract

To reduce the potential risks that may arise from the ADMIN contract, we advise implementing a multi-signature wallet to oversee its management. This will ensure that no single entity has complete control over the contract, thereby reducing the likelihood of malicious activity or mistakes that could result in loss of funds or compromised security.

Sensitive Data

We have taken measures to safeguard all sensitive data and private keys with the SIGNER role by storing them in an internal network that is not accessible from external sources. However, it is crucial to acknowledge that the overall security of the system also relies on the operating procedures defined for each role. To ensure optimal security, we recommend establishing clear protocols and designating specific individuals to be responsible for each role. This can help minimize the potential risks associated with the misuse of roles and ensure that all security measures are consistently followed.

2.3. Findings

During the audit process, the audit team found no vulnerable issue in the given version of Milady Meme Coin API Backend.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*May 16,2023*	Public Report	Verichains Lab

Table 3. Report versions history