Matrix Audit Report

Version 1.0

Zero Drift

December 23, 2025

Matrix Audit Report

Zero Drift

December 23, 2025

Prepared by: Zero Drift

Table of Contents

- About Zero Drift
- Disclaimer
- Risk Classification
- Protocol Overview
- Audit Scope
- Executive Summary
  - Summary
  - Issues Found
  - Summary of Findings
- Findings
  - Critical
  - High
  - Medium
  - Low
  - Informational
  - Gas

About Zero Drift

Zero Drift is a tech-driven Web3 auditing firm dedicated to zero-incident smart-contract assurance for mission-critical protocols.

Disclaimer

The Zero Drift team makes all effort to find as many vulnerabilities in the code in the given time period, but holds no responsibilities for the findings provided in this document. A security audit by the team is not an endorsement of the underlying business or product. The audit was time-boxed and the review of the code was solely on the security aspects of the Solidity implementation of the contracts.

Risk Classification

	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

Protocol Overview

Matrix is an ERC20 token project. The reviewed scope focuses on token ownership patterns and initial token distribution mechanics for the `Matrix` token contract.

Audit Scope

Repository and commit reviewed:

- MatrixonBNB/Matrix-token @ `8f237b5eaa8e608194098398114753b5b5531359`
  - Reference: https://github.com/MatrixonBNB/Matrix-token/commit/8f237b5eaa8e608194098398114753b5b
- Files of interest:
  - `MatrixToken.sol`

Executive Summary

Over a focused review, the Zero Drift team evaluated the Matrix token implementation with emphasis on ownership transfer safety and initial token distribution. Two minor (low-severity) issues were identified.

The first issue is fixed by adopting a two-step ownership transfer, and the second is acknowledged. The project uses a multisig wallet to mitigate centralization risk around token custody.

Overall, the code is straightforward and follows standard ERC20 patterns. The identified risks are primarily operational/centralization in nature rather than protocol-logic vulnerabilities.

Summary

Project Name	Matrix
Repository	https://github.com/MatrixonBNB/Matrix-token
Commit	8f237b5eaa8e608194098398114753b5b5531359
Audit Timeline	Dec 23, 2025
Methods	Manual Review

Issues Found

	Count
Critical Risk	0
High Risk	0
Medium Risk	0
Low Risk	2
Informational	0
Gas Optimizations	0
Total Issues	**2**

Summary of Findings

ID	Description	Status
L-1	Single-step ownership transfer can lead to misassignment	Resolved
L-2	Initial token distribution centralization risk	Acknowledged

Findings

Critical

None.

High

None.

Medium

None.

Low

L-1 Single-step Ownership Transfer Issue

Severity: Low

Description

- The contract used single-step ownership transfer via `Ownable(msg.sender)` in the constructor, which introduces risk of permanent loss of control if the new owner is mis-specified during transfer.

Impact

- Operational risk of owner misassignment or accidental loss of control over privileged functions.

Recommendation

- Adopt a two-step ownership transfer pattern (e.g., OpenZeppelin `Ownable2Step`) to require explicit acceptance by the new owner.

Status

- Resolved. The contract implements a two-step ownership transfer (e.g., Ownable2Step), addressing the risk.

L-2 Initial Token Distribution Centralization Risk

Severity: Low

Description

- All tokens are initially minted to `msg.sender` (e.g., `_mint(msg.sender, 200_000_000 * 10 ** decimals())`). This creates a centralization and custody risk during early stages of the token lifecycle.

Impact

- Compromise or misuse of the controlling address could enable large transfers or market impact, harming holders and liquidity.

Recommendation

- Maintain transparent distribution, consider timelocks or vesting for team/treasury allocations, and secure custody via robust operational controls (multisig, hardware keys, on-call procedures). Where feasible, split custody across multisig signers and consider time-delayed administrative actions.

Status

- Acknowledged. The team states they use a multisig wallet for custody to mitigate this risk. This reduces single-key compromise exposure, but residual centralization risk remains and should be managed through policy and process.

Informational

None.

Gas

None.