ETHOS AUDIT

Cleverminu

Audit Report

Sep. 29, 2022

Contents

Executive Summary

Audit Details

Project Name	Clever Minu
Codebase	https://polygonscan.com/address/0x155AB9Cd3655Aa6174E1e743a6DA1E208762b03d#code
Initial Audit Date	Sep. 28, 2022
Revision Dates	-
Methodology	Manual, Automated

Methodology

This audit's objectives are to evaluate:

- Security-related issues
- Code quality
- Relevant documentation
- Adherence to specifications
- Adherence to best practices

This audit examines the possibility of issues existing along the following vectors (but not limited to):

- Single & Cross-Function Reentrancy
- Front Running (Transaction Order Dependence)
- Timestamp dependence
- Integer Overflow and Underflow
- Mishandled exceptions and call stack limits
- Unsafe external calls
- Number rounding errors
- DoS with (Unexpected) Revert
- DoS with Block Gas Limit
- Insufficient gas griefing
- Forcibly sending native currency
- Logical oversights
- Access control
- Centralization of power
- Logic-Specification Contradiction
- Functionality duplication
- Malicious token minting

The code review conducted for this audit follows the following structure:

1. Review of specifications, documentation to assess smart contract functionality
2. Manual, line-by-line review of code
3. Code's adherence to functionality as presented by documentation
4. Automated tool-driven review of smart contract functionality
5. Assess adherence to best practices
6. Provide actionable recommendations

Results Summary

The CLEVERMINU token project has been audited by Ethos and has been given a **PASSING** grade.

The audit found several low risk and informational issues that don't require any changes due to their low impact on the overall security of the smart contract.

The contract also does not contain any backdoors or malicious code.

CLEVERMINU token details and project info can be found here: https://www.cleverminu.com/

Issues Reported

Severity	**Unresolved**	**Acknowledged**	**Resolved**
High	0	0	0
Medium	0	0	0
Low	0	1	0
Informational	0	3	0

Issues Summary

ID	**Title**	**Severity**	**Status**
CM-0	Unchecked transfer	Low	Reported
CM-2	Missing events	Info	Reported
CM-3	Block timestamp comparison	Info	Reported
CM-4	Public functions that could be external	Info	Reported

Detailed Findings

Code Documentation

The code contains minimal commenting.

Adherence to Specifications

The CLEVERMINU smart contract adheres to the smart contract functionality described by the project documentation and is in line with its intended usage.

Adherence to Best Practices

The CLEVERMINU smart contract adheres to the best practices associated with a standard EVM compatible Solidity smart contract.

CM-0 – Unchecked transfer

Severity: Low **Status**: Reported

Description: The return value of an external transfer/transferFrom call is not checked.

Risk: Several tokens do not revert in case of failure and return false. If one of these tokens is used, deposit will not revert if the transfer fails, and an attacker can call deposit for free.

Recommendation: Use SafeERC20, or ensure that the transfer/transferFrom return value is checked.

CM-1 – Missing events

Severity: Info **Status:** Reported

Description: Missing events for critical arithmetic parameters.

Risk: If execution of functions which update state variables do not emit events, they cannot be tracked by dApps which may rely on success/failure of such calls.

Recommendation: Emit an event for critical parameter changes.

CM-2 – Block timestamp comparison

Severity: Informational **Status**: Reported

Description: Some functions use a statements that relies on a block timestamp comparison.

Risk: Miners can manipulate block.timestamp value to exploit the require statement and contract.

Recommendation: Avoid using block.timestamp for comparison logic.

CM-3 – Public functions that could be external

Severity: Informational **Status**: Reported

Description: Public functions that are never called by the contract should be declared external to save gas.

Risk: Gas optimization

Recommendation: Use the external attribute for functions never called from the contract.