SMART CONTRACT SECURITY AUDIT

SolidityLabs

MidasDAO(CROWN)

On December 19, 2021, **SolidityLabs** received an application for a smart contract security audit of **MidasDAO(CROWN)**. This smart contract security audit yielded the following results:

Token Name: $CROWN

Contract address: 0xed46443C18E38064523180Fc364C6180b35803d3

Link Address:
https://snowtrace.io/address/0xed46443C18E38064523180Fc364C6180b35803d3

The audit items and results:
(The audit responsibility scope does not include other unknown security vulnerabilities.)

Audit Result: Passed

Ownership: Not renounced
(The contract contains ownership functionality and ownership is not renounced which allows the creator or current owner to modify contract behavior)

KYC Verification: Not verified

Audit Number: SLA0000000001
Audit Date: December 20, 2021
Audit Team: SolidityLabs
https://www.SolidityLabs.io

Table of Content

Introduction

The purpose of this audit is to assess the overall security of **MidasDAO(CROWN)** Smart Contract. The purpose of this report is to ensure the reliability and correctness of their smart contracts by reviewing their system's architecture and the smart contract codebase completely and rigorously.

During our rigorous testing of the project, the SolidityLabs team reviewed the smart contract architecture to ensure that it is structured and that it uses third-party smart contracts and libraries in a safe way.
In our team's next step, we examined the Smart Contract line by line for any potential issues such as race conditions, timestamp-dependent transactions, or denial of service attacks.
To ensure that each function in the contract works as expected, we coded/conducted custom unit tests for each function within the contract. In Automated Testing, we identified vulnerabilities and security flaws by using tools we developed in-house. Several of our team members collaborated on testing the code, including:

- Testing the functionality of the Smart Contract to determine proper logic has been implemented throughout the entire process.
- Analyzing the code's complexity in depth and conducting a detailed, line-by-line review.

Running live tests using multiple clients to deploy the code on testnet.
Checking how Smart Contracts perform in case of bugs and vulnerabilities by analyzing failure preparations.

- Verifying that all libraries used in the code are up-to-date.
- Analyzing the security of the on-chain data.

Audit Details
Project Name: MidasDao(CROWN)
Website: https://midasdao.org/
Languages: Solidity (Smart contract)
Platforms and Tools: Remix IDE, Contract Library, Mythril, Solhint, Ganache, Truffle, TruffleTeam, VScode

Audit Goals

In the audit, the focus was on verifying that the Smart Contract System was secure, resilient, and working according to specification. The audit activities can be divided into three categories:

Security
Identifying security related issues within each contract and the system of contract.

Sound Architecture
Evaluation of the architecture of this system through the lens of established smart contract best practices and general software best practices.

Code Correctness and Quality

A full review of the contract source code. The primary areas of focus include:

- Accuracy
- Readability
- Sections of code with high complexity
- Quantity and quality of test coverage

Issue Categories
Every issue in this report was assigned a severity level from the following:

High level severity issues
Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium level severity issues
Issues on this level could potentially bring problems and should eventually be fixed.

Low level severity issues
Issues on this level are minor details and warnings that can remain unfixed but would be better fixed at some point in the future.

Number of issues per severity

Critical	High	Medium	Low	Note
0	0	0	0	0

Issues Checking Status

№	Issue description.	Checking status
1	Compiler warnings.	Passed
2	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3	Possible delays in data delivery.	Passed
4	Oracle calls.	Passed
5	Front running.	Passed
6	Timestamp dependence.	Passed
7	Integer Overflow and Underflow.	Passed
8	DoS with Revert.	Passed
9	DoS with block gas limit.	Passed
10	Methods execution permissions.	Passed
11	Economy model.	Passed
12	The impact of the exchange rate on the logic.	Passed
13	Private user data leaks.	Passed
14	Malicious Event log.	Passed
15	Scoping and Declarations.	Passed
16	Uninitialized storage pointers.	Passed
17	Arithmetic accuracy.	Passed
18	Design Logic.	Passed
19	Cross-function race conditions.	Passed
20	Safe Zeppelin module.	Passed
21	Fallback function security.	Passed

Manual Audit:

Our developers tested/read the code line by line for this section. To test the contract functionality, we also used Remix IDE's JavaScript VM and Kovan networks.

Critical Severity Issues

No critical severity issues found.

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

No low severity issues found.

Automated Audit

Remix Compiler Warnings

It throws warnings by Solidity’s compiler. If it encounters any errors the contract cannot be compiled and deployed. **No issues found.**

Disclaimer

In this report, we discuss our findings, which are based on our analysis, in accordance with good industry practice as of the date of this report, in relation to cybersecurity and issues in the framework and algorithms for smart contracts. Details are provided in this report. To gain a full understanding of our analysis, it is imperative that you read the full report. In conducting our analysis and producing this report, we have done our very best. However, you should not rely on it and cannot make a claim against us based solely on what it says or does not say, or how it was produced. In addition, it is important for you to conduct your own independent investigations before making any final decisions. In the disclaimer below, we go into more detail on this - please read it carefully.

DISCLAIMER: By reading this report or any part of it, you agree to its terms. In the event that you do not agree to the terms, stop reading this report immediately, and delete and destroy all copies of this report that you have downloaded and/or printed. This report is provided for informational purposes only and does not constitute investment advice. Any reliance on the report or its contents is void, and **SolidityLabs** and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and others) are not responsible for any errors or omissions contained in the report. **SolidityLabs** owes no duty of care to you or anyone else, nor does **SolidityLabs** make any warranty or representation regarding the accuracy or completeness of the report. As such, **SolidityLabs** is providing the report "as is", without any conditions, warranties, or other terms of any kind, except as set out in this disclaimer, and **SolidityLabs** excludes all representations, warranties, conditions, and other terms (including, without limitation, the implied warranties of satisfactory quality and fitness for purpose) which might otherwise apply to the report had this clause not been included. Except & only to the extent that it is prohibited by law, **SolidityLabs** hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against **SolidityLabs**, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

Security analysis is purely based on smart contracts. There was no review of applications or operations. The code of the product was not examined.

Summary

MidasDAO(CROWN) contract does not contain any high severity issues!

Note:

Note that the audit does not make any statements or warranties regarding business model, investment attractiveness, or code sustainability. The report focuses on the only contract mentioned.