Decentralizing the World

DREGN SMART CONTRACT

FINAL AUDIT REPORT - JULY 2023

Table of Content

Summary

This is a limited audit report based on our analysis of the Dregn Smart Contract. It covers industry best practices as of the date of this report, concerning: smart contract best coding practices, cybersecurity vulnerabilities. (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

Smart contracts are deployed and executed on the blockchain. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks.

You are advised to read the full report to get a full view of our analysis. While we did our best in producing this report, it is important to note that you should not rely on this report, and cannot claim against us, based on what it says or does not say, or how we produced it, and you need to conduct your independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy all copies of this report downloaded and/or printed by you.

The report is provided "as it is" without any condition, warranty, or other terms of any kind except as set out in this disclaimer. Team Antier Solutions hereby excludes all representations, warranties, conditions, and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose, and the use of reasonable care and skill) which, but for this clause, might affect the report.

DREGN commissioned Antier Solutions to perform an end-to-end source code review of their Solidity Smart Contract. Team Antier Solutions performed the audit from 20th July to 27th July 2023.

The following report discusses severity issues and their scope of rectification through change recommendations. It also highlights activities that are successfully executed and others that need total reworking (if any).

The report emphasises best practices in coding and the security vulnerabilities if any.

The information in this report should be used to understand the overall code quality, security, and correctness of the Smart Contract. The analysis is static and entirely limited to the Smart Contract code.

Overview

Project Overview

Project Name	DREGN
Status	Pre Deployment
Language	Solidity
Code Repo.	

Audit Details

Audit Date	20-July-2023
Tools Used	Slither, Mythril and manual
Audit Type	New audit
Initial Commit	217c664f
Fix Commits	**Commit** / **Commit Hash**: e6561357 / e6561357fd312d4443f26867d1240842110f8795
Audit Scope	**File** / **Status**: ICO.sol / Moderately Vulnerable; Vesting.sol / Safe; Dregn.sol / Safe

Vulnerability Summary

	High Difficulty	Medium Difficulty	Low Difficulty	Not exploitable
Highly vulnerable	0	0	0	0
Medium vulnerability	0	0	0	0
Low vulnerability	0	0	0	1
Optimizational Errors	0	0	0	2

Vulnerabilities found

Sr. No.	Vulnerability	Severity	Status
01	Randomness of referral code	Low	Fixed

01 Randomness of referral code

Vulnerability Details

Severity	Difficulty	Location	Status
Low	Low	ICO.sol	Fixed

Syntax

```
function random() internal returns (uint) {
    counter++;
    return
        uint(
            keccak256(
                abi.encodePacked(
                    block.timestamp,
                    block.difficulty,
                    msg.sender,
                    counter
                )
            )
        ) % 36;
}
```

Description

Randomness from the block.timestamp can be predicted and can be manipulated by the miners.

Recommendation

Use a strong source of randomness such as an oracle.

Optimizations

Sr. No.	Title	Severity	Status
01	Extensive use of msg.sender	Optimisation	Fixed
02	Variable declaration	Optimisation	Fixed

01 Extensive use of msg.sender

Vulnerability Details

Severity	Difficulty	Location	Status
Optimisation	Not Exploitable	ICO.sol and Vesting.sol	Fixed

Description

Repeated reading of global variables such as Msg.Sender along with a write operation costs higher gas.

Recommendation

We recommend using a local variable to store the value & reusing it in the scope.

02 Variable Declaration

Vulnerability Details

Severity	Difficulty	Location	Status
Optimisation	Not Exploitable	Vesting.sol	Fixed

Description

No setter function for Marketing, Ecosystem, Treasury, Team and Advertised addresses.

Recommendation

Above addresses can be kept constant if you don't want to change in future.

Technical Analysis

We checked Dregn Smart Contracts for commonly known and specific business logic vulnerabilities. Following is the list of vulnerabilities tested in the Smart Contract code:

Vulnerability	Results	CounterMeasure Used
Reentrancy	passed	OpenZeppelin Reentrancy contract
Timestamp Dependence	N/A	-
Race Condition	passed	-
Use of TX. Origin	pass	N/A
Gasless send	N/A	N/A
Balance equality	Pass	-
Nested array	pass	N/A
Unchecked external call	Pass	-
Mathematical errors	Pass	-
Using var	N/A	N/A
Private modifier	Pass	-
Locked money	Pass	-
Integer overflow/underflow	Pass	Solidity version 0.8.0+
Address hardcoded	Pass	-
Implicit visibility level	Pass	-

Limitations on Disclosure and Use of this Report

This report contains information concerning potential details of Dregn and methods for exploiting them. Antier Solutions recommends that precautions should be taken to protect the confidentiality of this document and the information contained herein.

Security Assessment is an uncertain process based on experiences, currently available information, and known threats. All information security systems, which by their nature are dependent on human beings, are vulnerable to some degree. Therefore, although Antier Solutions has identified major security vulnerabilities in the analysed system, there can be no assurance that any exercise of this nature will identify all possible vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate those exposures.

As technologies and risks change over time, the vulnerabilities associated with the operation of the Dregn Smart Contract described in this report, as well as the actions necessary to reduce the exposure to such vulnerabilities will also change. Antier Solutions makes no undertaking to supplement or update this report based on the changed circumstances or facts of which Antier Solutions becomes aware after the date hereof.

This report may recommend that Antier Solutions use certain software or hardware products manufactured or maintained by other vendors. Antier Solutions bases these recommendations on its prior experience with the capabilities of those products. Nonetheless, Antier Solutions does not and cannot warrant that a particular product will work as advertised by the vendor, nor that it will operate in the manner intended.

The Non-Disclosure Agreement (NDA) in effect between Antier Solutions and Dregn governs the disclosure of this report to all other parties, including product vendors and suppliers.