STAYSAFU
AUDIT

August 22ND, 2022

ETHDAO

TABLE OF CONTENTS

AUDIT SUMMARY

This report was written for ETHDAO ($ETHDAO) in order to find flaws and vulnerabilities in the ETHDAO project's source code, as well as any contract dependencies that weren't part of an officially recognized library.

A comprehensive examination has been performed, utilizing Static Analysis, Manual Review, and ETHDAO Deployment techniques. The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors
- Assessing the codebase to ensure compliance with current best practices and industry standards
- Ensuring contract logic meets the specifications and intentions of the client
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders
- Through line-by-line manual review of the entire codebase by industry expert

AUDIT OVERVIEW

PROJECT SUMMARY

Project name	ETHDAO
Description	The birth of ETHDAO is a perfect solution to the loopholes on the original ETH, and at the same time it is more secure and reliable to protect the financial assets of cryptocurrency investors.
Platform	BNB Chain
Language	Solidity
Codebase	https://bscscan.com/address/0xcf0d97ca38ac4e89b7ad4ec4d98752a5bc064583#code#L1

FINDINGS SUMMARY

Vulnerability	Total
Critical	0
Major	0
Medium	4
Minor	1
Informational	0

EXECUTIVE SUMMARY

There have been no major or critical issues related to the codebase and all findings listed here range from informational to medium. The medium security issues are the dependence on a decentralized exchange platform, centralization of privileges, missing threshold checks and initial token supply.

AUDIT FINDINGS

Code	Title	Severity
CENT-1	Centralization of major privileges	Medium
CENT-3	Centralization of initial token distribution	Medium
EXT-1	Dependence to external protocol	Medium
THRE-3	Missing threshold checks	Medium
BLOC-2	Use of block.timestamp	Minor

CENT-1 | Centralization of major privileges

Description

The onlyOwner modifier of the smart contract(s) gives major privileges over it (change fees)*. This can be a problem, in the case of a hack, an attacker who has taken possession of this privileged account could damage the project and the investors.
*This list is not exhaustive but presents the most sensitive points

Recommendation

We recommend at least to use a multi-sig wallet as the owner address, and at best to establish a community governance protocol to avoid such centralization. For more information, see https://solidity-by-example.org/app/multi-sig-wallet/

CENT-3 | Centralization of initial token distribution

Description

A constructor (line 454) within the contract mints the initial token supply to the passed parameter address (ReceiveAddress). This initially centralizes token supply to the deployer address.

Recommendation

We recommend decentralizing tokens as soon as possible, matching the project's intentions. Examples of this are burning tokens or adding tokens to a liquidity pool (locked). We also recommend being fully transparent with the community about token distribution.

EXT-1 | Dependence to external protocol

Description

The contract interacts with PancakeSwap protocols. The scope of the audit would treat these third party entities as black boxes and assume they are fully functional. However in the real world, third parties may be compromised thus leading assets to be lost or stolen. We fully understand that the business logic of the ETHDAO project is designed to work with PancakeSwap protocols. This extends to other protocols and interfaces not within the scope of this audit.

Recommendation

We encourage the team to constantly monitor the security level of the entirety of PancakeSwap protocols interacted with, as the security of the project is highly dependent on the security of these decentralized exchange platforms.

THRE-3 | Missing threshold checks

Description

Functions which can change sensitive variables within ETHDAO's contract do not contain threshold checks to ensure these variables are not changed to unreasonable values. This includes fees. As such it is important to add a threshold to prevent an attacker from fees as 100% easily. Key examples of Identified functions with this issue have been listed below:

- setDistributionSettings -> Line 540

Recommendation

We recommend adding threshold checks using require statements for each of the identified functions above and other functions with this issue.

BLOC-2 | Use of block.timestamp

Description

The use of block.timestamp can be problematic. The timestamp can be partially manipulated by the miner (see https://cryptomarketpool.com/block-timestamp-manipulation-attack/).

Recommendation

We fully understand that the use of block.timestamp within the ETHDAO Protocol is required for certain functionality. Nevertheless, it is still useful to point out this kind of potential security problem.

DISCLAIMER

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement.

This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement.

This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without StaySAFU's prior written consent.This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts StaySAFU to perform a security assessment.

This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with

any particular project.

This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk.

StaySAFU's position is that each company and individual are responsible for their own due diligence and continuous security. StaySAFU's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or fun.