AEGIS

SMART CONTRACTS SECURITY ASSESSMENT

Project: Dex Finance
Date: 20th June 2022

Copyright © 2022 Aegis Audits

TABLE OF CONTENTS

ABOUT AEGIS

Aegis Audits conducts a comprehensive security review of blockchain applications, using modern tools and employing only the most experienced solidity experts on the market. During the elaboration of the audit, auditors analyze possible attack vectors both from the project owners and its users and rate them by Severity (see Appendix A) from Informational to Critical as per common reason, giving an adequate explanation in the body of the audit. Our Audits are versioned, and clients get a grace period to alleviate or comment on all of our findings.

We are becoming the one-stop shop for blockchain cybersecurity, protecting investors all around the world from fraudulent behavior. And with our revolutionary Aegis Audits' NFT IPO, every investor and protocol around the world is now able to participate in our econom-ic success, as 80 % of profits are distributed in dividends to our NFT holders.

Website: https://aegisaudits.com/
E-Mail: aegisaudits@gmail.com
Discord: https://discord.gg/aegisaudits
Twitter: https://twitter.com/aegisaudits
Telegram: https://t.me/aegisaudit

METHODOLOGY

As per standard code review practices, we use manual and static analysis. During the manual phase, auditor(s) review source code line-by-line, studying its intended and actual behavior, referencing known vulnerabilities (including SWC Registry https://swcregistry.io/), comparing the code to common contracts, and noting all things that are out of the ordinary for confirmation or rejection. Static analysis refers to a computer-aided analysis of the code, providing automatized and powerful insight into additional subtle issues possibly present in the code.
Some auditors additionally write their own test cases and try to break the contracts in their own local simulated blockchain environment. This is called dynamic analysis and is often employed in the more complex contracts, where consolidated testing scenarios help assess the completeness of contract logic or reversely give a proof-of-concept for potential security vulnerability.
Finally, all auditors do on-chain verification of live contracts. This crucial step confirms con-tracts were not swapped for malicious only after audit, or that parameters are set based on reasonable expectations. Issues such as non-renounced ownerships are also assessed in this step.

PROJECT DETAILS

Project Name	Dex Finance
Description	DEX Finance is a decentralized autonomous organization (DAO) providing an ecosystem of financial products that aims at providing safe and sustainable yields. Their core products consist of the DEX Money Market, dexIRA & dexETF.
Links	Website: https://www.dexfinance.com/ Twitter: https://twitter.com/DexFinance Telegram: https://t.me/dexfinance Discord: https://discord.com/invite/DexFinance
Code Language	Solidity
Chain	Binance Smart Chain (56)

VERSION DETAILS

Version	Based on status at	Published at	Elaborated by	Notes
v1.0	20th June 2022	20th June 2022	Filip	Initial version

OBJECTS OF REVIEW

In Version	Source	Contents
v1.0	On-chain live contracts	SingleStakingRewardPool `0xd69db827939e26511068aa2bf742e7463b292190`

SUMMARY

FINDINGS

Type	Total	Fully resolved	Partially Resolved	Acknowledged	Open
Critical					
Major					
Medium					
Minor	1				1
Informational	1				1

The reviewed contract matches its profile as an incentivized staking contract.

We have not found any security vulnerabilities in the contract.

The minor issue is connected to owner privileges. Nonetheless, Dex Finance team has chosen to retain higher control of its contracts to assure maximum flexibility when reacting to market conditions in rest of the protocol, including core contracts. Privilege risk in this specific pool is thus very low.

To completely assess the report, we recommend reading the full Findings section.

AUDIT PROCEDURE

Auditors	Filip
Audited as	Fork of Tomb Finance, reward pool contract
Methodology	The audit focused on the SingleStakingRewardPool contract. Dex Finance has several independent audits executed for other portions of their protocol: https://www.dexfinance.com/audits/
Tools	VSCode https://bscscan.com

Aegis Audits has no control over website UI that projects provide. Always double check you are signing a contract matching one of the contracts in section Objects of Review.

Aegis Audits concerns itself exclusively with code quality and smart contract security. We have not audited tokenomics, nor a general likelihood of making money with this project. Aegis report is not financial advice.

FINDINGS

Finding ID	R-001	**Severity**	Minor
Type	Centralization / Privilege	**Status**	Open

Location	SingleStakingRewardPool
Description	Owners can set fees up to 20%, drain reward token, force people to withdraw 5 days after pool ends, drain deposited tokens 10 days after pool ends, and prolong pool end time. *Note: if fees are set high, users can choose to bypass them, forgoing the rewards, through* `emergencyWithdraw` *function.*
Recommendation	Ensure safe handling of the owner wallet, possibly use a timelock / multisignature, or renounce contract.
Alleviation	

Finding ID	R-002	**Severity**	Informational
Type	Style	**Status**	Open

Location	SingleStakingRewardPool
Description	Based on the intended use with only a single reward pool, some redundant leftover code from share reward contract remains, such as repeated code in `forceWithdraw`, redundant function `massUpdatePools`, `checkPoolDuplicate` function, `onlyOwner` modifiers in `private` functions, and any and all cycles through pools.
Recommendation	Resolving this finding is optional and based on the temporary nature of the contract, possibly counter-productive.
Alleviation	

APPENDIX A: ISSUE SEVERITY CLASSIFICATION

The Auditor(s) assign one of the following Severities to every finding as per common practice.

Critical. Such issues may result in significant loss of funds, complete contract logic breakdown, or the ability of project owners to withdraw liquidity in an unreasonable way. Code snippets proving the project owner's malicious intent are flagged as critical as well. Critical issues require immediate attention, and investing in projects with critical issues is extremely risky. Examples include unguarded mint functions or their executions, provably illicit pool drainage logic, or potential flash-loan vulnerabilities.

Major. Although not proving malicious intent by themselves, major issues may still be exploited by project owners or users for a significant loss of funds or very irregular contract behavior. Examples include centralized ownership without Timelocks and multi-signatures, potential reentrancy vulnerabilities, and concentrated holdings of tokens.

Medium. Such issues do not pose an immediate and severe risk but may pose a risk of partial loss of funds or irregular contract behavior. Examples include susceptibility to obviously unintended investment strategies, high-impact integer overflows, or high-impact standardization faults such as library usage.

Minor. These issues pose a low risk to contract logic or investor funds but may be convenient to consider. Examples include integer overflows in non-essential places, non-versioned libraries, missing or faulty licensing, misleading function names, or low-impact standardization mistakes.

Informational. These issues do not pose any risk to contract logic and investor funds. Examples include tokenomics clarifications, gas optimizations, redundant code, misleading comments, style, and convention. Common development practices such as comments, test suites, and git best practices are also evaluated.

Confirmational. In specific situations, we issue these findings, which confirm some of the universally-concerning facts that many investors seek. Examples include contract renounces and confirmation of a contract being fork of another protocol. Note: These points are not actual issues. Obviously, only a small subset of tests ran in an audit suite receives its Confirmational Finding. Note: *These points are not actual issues. Obviously, only a small subset of tests ran in an audit suite receives its Confirmational Finding*.

APPENDIX B: DISCLAIMER

This audit is for informational purposes only and does not provide any financial or investment advice. This report does not substitute, in any way, due diligence and your own research. This report represents result extensive process intending to help our customers improve quality of their code and readers to assess quality of customers‘ code, but should not be used in any way to make decisions around involvement in any particular project.

Audit has been done in accordance to methodology as outlined in About Aegis and Audit Procedure sections Unless explicitly and specifically stated, only code quality has been reviewed, focusing on security flaws which could cause loss of funds or logical breakdowns within the contracts. Unless explicitly stated, tokenomics have not been reviewed (although in cases of forks of one project, Auditor may point out cases of significant deviations from common settings). Website UI has not been reviewed, as it is impossible for any auditing body to assure security of domains which are under absolute control of owners – always check you are signing correct contracts.

The report does not signify an „approval,“ „endorsement,“ or „disapproval“ of the Project. The audit does not indicate in any way your likelihood of making, or not losing, money in the project, as we have no control over issues such as general viability of financial primitives presented, their tokenomics, and actions of project owners including, but not limited to, selling their positions or abandoning the project.

The audit has been based on status dated in section Version Details, on artifacts detailed in Objects of Review. Specifically, we have no control nor knowledge of changes made after the date, or on different artifacts. In case the Objects of Review are not live contracts, but private code or GitHub repositories, we expect these artifacts to be full, unaltered, unabridged, and not misleading.

The audit has been elaborated by paid professional(s) as mentioned in section Audit Procedure. Please note that all statements made in this report are Auditor(s)’ and do not reflect stance of © Aegis Audits itself.

This report is published by © Aegis Audits and is under © Aegis Audits sole ownership. It may not be transmitted, disclosed, modified, referred to, or relied upon by any person for any purposes without © Aegis Audits prior written consent.