

STAYSAFU **AUDIT**

August 25TH, 2022

Fundex

TABLE OF CONTENTS

- I. SUMMARY
- II. OVERVIEW
- III. FINDINGS
 - A. **CENT-1** | Centralization of major privileges
 - B. **CENT-3** | Centralization of initial token distribution
 - C. **EXT-1** | Dependence to external protocol
 - D. **THRE-3** | Missing threshold checks
 - E. **MSG-1** | Missing event emits
- VI. DISCLAIMER

AUDIT SUMMARY

This report was written for Fundex (\$FDX) in order to find flaws and vulnerabilities in the Fundex 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 Fundex 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	Fundex
Description	Fundex.fund is decentralized crypto exchange and Equity crowdfunding Recent developments in DeFi have created exponential value for cryptocurrency and tokens, by adding new and innovative technology solutions that allow for "old world capital market activities" like lending, borrowing, and securitization to digital assets as well as the new digital era market making infrastructure.
Platform	BNB Chain
Language	Solidity
Codebase	https://bscscan.com/address/0x8235868aDB63394728c82338160fd80D7dDD28a3#code

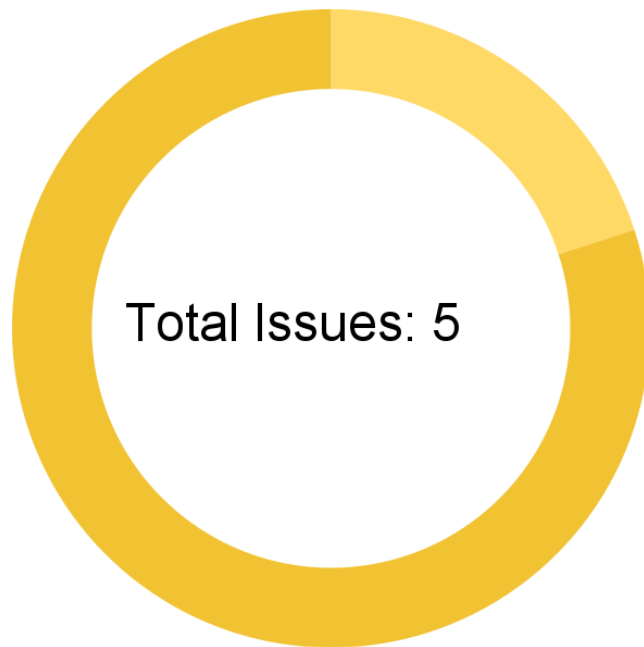
FINDINGS SUMMARY

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 include: the dependence on a decentralized exchange platform, centralization of privileges, and missing threshold checks.

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
MSG-1	Missing event emits	● Minor

CENT-1 | Centralization of major privileges

Description

The **onlyOwner** modifier of the smart contract(s) gives major privileges over it (**change buy fees, change sell fees, set max tx amount**)*. 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** within the contract mints the initial token supply to the deployer address (`msg.sender`). 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 **Fundex** 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 Fundex's contract do not contain threshold checks to ensure these variables are not changed to unreasonable values. This includes fees and max tx amount. As such it is important to add a threshold to prevent an attacker from setting max transaction amount as 0 or fees as 100% easily. Key examples of Identified functions with this issue have been listed below:

- ❖ `setMaxTxAmount` -> Line 1199
- ❖ `setLiquidityFeePercent` -> Line 1195
- ❖ `setTaxFeePercent` -> Line 1191

Recommendation

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

MSG-1 | Missing event emits

Description

Some functions within Fundex's contracts modify sensitive variables without emitting an event. Functions with this issue are listed below:

- ❖ `setMaxTxAmount` -> Line 1199
- ❖ `setLiquidityFeePercent` -> Line 1195
- ❖ `setTaxFeePercent` -> Line 1191

Recommendation

We recommend amending these functions to include event emits to ensure transparency with users.

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.