AUDITS

SECURITY ASSESSMENT

# FLUXUS FINANCE

SEPTEMBER 22ND 2022

# TABLE OF CONTENTS

# LEGAL DISCLAIMER

**MH Audits are not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. These reports are 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 MH Audits to perform a security review.**

**MH Audits 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.**

MH Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

The report is provided only for the contract(s) mentioned in the report and does not include any other potential additions and/or contracts deployed by Owner. The report does not provide a review for contract(s), applications and/or operations, that are out of this report scope.

**MH Audits' 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 functionality of the technology we agree to analyze.**

MH Audits represents an extensive auditing 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. MH Audits' position is that each company and individual are responsible for their own due diligence and continuous security.

The security audit is not meant to replace functional testing done before a software release. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent manual audits and a public bug bounty program to ensure the security of the smart contracts.

# INTRODUCTION

**MH Audits is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.**

### Secure your project with MH Audits

We offer field-proven audits with in-depth reporting and a range of suggestions to improve and avoid contract vulnerabilities.

Industry-leading comprehensive and transparent smart contract auditing on all public and private blockchains.

### Vunerability checking

A crucial manual inspection carried out to eliminate any code flaws and security loopholes. This is vital to avoid vulnerabilities and exposures incurring costly errors at a later stage.

### Contract verification

A thorough and comprehensive review in order to verify the safety of a smart contract and ensure it is ready for launch and built to protect the end-user.

### Risk assessment

Analyse the architecture of the blockchain system to evaluate, assess and eliminate probable security breaches. This includes a full assessment of risk and a list of expert suggestions.

### In-depth reporting

A truly custom exhaustive report that is transparent and depicts details of any identified threats and vulnerabilities and classifies those by severity.

### Fast turnaround

We know that your time is valuable and therefore provide you with the fastest turnaround times in the industry to ensure that both your project and community are at ease.

### Best-of-class blockchain engineers

Our engineers combine both experience and knowledge stemming from a large pool of developers at our disposal. We work with some of the brightest minds that have audited countless smart contracts over the last 4 years.

# PROJECT SUMMARY

## PROJECT INTRODUCTION

**The ultimate DeFi suite on NEAR. Aggregate yield, swaps, data, NFTs & take your DeFi investments to the next level. Fluxus Finance is the first NEAR-native yield aggregator, auto-compounder, and yield optimizer. By leveraging Near's scalability, Fluxus can implement faster compounding periods as well as more complex vault strategies with no significant usage fees.**

Fluxus has established a bold roadmap of integrating on-ramp payments across the world, NEAR to Aurora native transactions, putting out more complex vault strategies (lending, hedging, stable-specific), and many other features, such as powerful and comprehensive dashboards, portfolio analytics and more to come.

**Project Name** *Fluxus Finance*

**Contract Name** -

**Contract Address** -

**Contract Chain** *Not Yet Deployed on Mainnet*

**Contract Type** *Smart Contract*

**Platform** *Near*

**Language** *Rust*

**Codebase** *Private Repository*

## INFO & SOCIALS

**Network** *Near Protocol (NEAR)*

**Website** *https://www.fluxus.finance/*

**Twitter** *https://twitter.com/FluxusFi*

**Telegram Chat** *https://t.me/fluxusfi*

**Telegram Ann** -

**Discord** *https://discord.gg/Z5fA7PuZ4R*

**Instagram** *https://www.instagram.com/fluxusfi/*

**Medium** *https://medium.com/fluxusfi*

**GitHub** *https://github.com/Fluxus-Finance*

**NearScan** -

# AUDIT SCORES


| Issues | 2 |
|---|---|
| Critical | 0 |
| Major | 0 |
| Medium | 1 |
| Minor | 1 |
| Informational | 0 |
| Discussion | 0 |

All issues are described in further detail on the following pages.

# AUDIT SCOPE

| FILE | LOCATION |
| --- | --- |
| fluxus-contracts/fluxus-treasurer/src/ external_contracts.rs<br>lib.rs<br>managed_tokens.rs<br>stakeholders.rs | *GitHub Repository* |
| fluxus-contracts/fluxus-safe/tests/ general.rs<br>jumbo_general.rs<br>utils.rs | *GitHub Repository* |
| fluxus-contracts/fluxus-safe/src/ account_deposit.rs<br>actions_of_strat.rs<br>admin_fee.rs<br>callback.rs<br>errors.rs<br>external_contracts.rs<br>fluxus_strat.rs<br>lib.rs<br>multi_fungible_token.rs<br>owner.rs<br>storage_impl.rs<br>token_receiver.rs<br>utils.rs<br>views.rs | *GitHub Repository* |

# AUDIT SCOPE

| FILE | LOCATION |
| --- | --- |
| fluxus-safe/src/jumbo/ jumbo_auto_compound.rs<br>jumbo_auto_compounder.rs<br>mod.rs | *GitHub Repository* |
| fluxus-safe/src/pembrock/ mod.rs<br>pembrock_actions_of_compounder.rs<br>pembrock_auto_compounder.rs | *GitHub Repository* |
| fluxus-safe/src/ref_finance actions_of_compounder.rs<br>auto_compound.rs<br>auto_compounder.rs<br>mod.rs<br>stable_auto_compound.rs<br>stable_auto_compounder.rs | *GitHub Repository* |

# REVIEW METHODOLOGY

## TECHNIQUES

**This report has been prepared for Fluxus Finance to discover issues and vulnerabilities in the source code of the Fluxus Finance project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Dynamic, Static Analysis and Manual Review 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 producedby industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from major to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective in the comments below.

## TIMESTAMP

| | |
|---|---|
| **Version** | v1.0 |
| **Date** | 2022/09/10 |
| **Description** | Layout project<br>Architecture / Manual review / Static & dynamic security testing<br>Summary |
| **Version** | v1.1 |
| **Date** | 2022/09/22 |
| **Description** | Reaudit addressed issues<br>Final summary |

# KEY FINDINGS

| TITLE | SEVERITY | STATUS |
| --- | --- | --- |
| Outdated and Vulnerable Crates | Minor | *Fixed* |
| Missing Overflow and Underflow Checks | Medium | *Fixed* |

***Description:***

*The Fluxus contracts were using multiple crates which were found to be outdated, unmaintained or were vulnerable to publicly disclosed CVEs. The following crates were affected:*

***Affected Crates:***

time - ***0.1.44***
ansi_term - ***0.12.1***
failure - ***0.1.8***

***Impacts:***

***The crates are affected by CVEs such as*** CVE-2020-26235 ***and*** CVE-2020-25575***.***

***Issue:*** *Outdated and Vulnerable Crates*

***Type:*** *Using components with know vulnerabilities*

***Level:*** *Minor*

***Remediation:*** *Update the crates to their latest versions if available or if the crates are not maintained anymore, it is recommended to switch to a different crate.*

***Alleviation / Retest:*** *The affected crates have been updated . The team responded with the following transcript:*

*it's a dependency from that crate and we are only using it to enable our testing environment so it won't be a dependency to our production build.*

***Description:***

*The Fluxus safe and treasurer contracts are not using checked arithmetic for doing calculations. This might allow the values to be over or under flowed and calculated incorrectly.*

*These issues occur when an arithmetic value is stored inside a variable but outside the variable's range which overflows or underflows the calculation and the values are reset back to either their minimum or maximum values.*

***Affected Crates:***

*All the arithmetic calculations*

***Impacts:***

*Allowing integer overflows and underflows may result in incorrect caculatins for tokens and other integer values.*

***Issue:*** *Missing Overflow and Underflow Checks*

***Type:*** *Overflow and Underflows*

***Level:*** *Medium*

***Remediation:*** *It is recommended to use* [overflow-checks=true] *in the Cargo.toml file. This will allow rust to automatically validate the arithmetic operations for overflows and underflows.*

***Reference:*** *https://doc.rust-lang.org/cargo/reference/profiles.html?highlight=overflow-checks#overflow-checks*

***Alleviation / Retest:*** *The Fluxus Finance team heeded our references and applied the suggested remediation.*

*Private GitHub Repository*

## FINDING CATEGORIES

The assessment process will utilize a mixture of static analysis, dynamic analysis, in-depth manual review and/or other security techniques.

This report has been prepared for Fluxus Finance project using the above techniques to examine and discover vulnerabilities and safe coding practices in Fluxus Finance's smart contract including the libraries used by the contract that are not officially recognized.

A comprehensive static and dynamic analysis has been performed on the solidity code in order to find vulnerabilities ranging from minor gas optimizations to major vulnerabilities leading to the loss of funds.

Various common and uncommon attack vectors will be investigated to ensure that the smart contracts are secure from malicious actors. The testing methods find and flag issues related to gas optimizations that help in reducing the overall gas cost It scans and evaluates the codebase against industry best practices and standards to ensure compliance It makes sure that the officially recognized libraries used in the code are secure and up to date.

## AUDIT SCORES

MH Audits AuditScores is not a live dynamic score. It is a fixed value determined at the time of the report issuance date.

**MH Audits AuditScores are not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. These reports and scores are 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 MH Audits to perform a security review.**

AUDITS

WEBSITE
MHAUDITS.IO

TWITTER
@MHAUDITS