StartFi Audit Report

Version 1.0.0

Serial No. 2021101400022015

Presented by Fairyproof

October 14, 2021

FAIRYPROOF

01. Introduction

This document includes the results of the audit performed by the Fairyproof team on the StartFi project, at the request of the StartFi team.

Audit Start Time:

September 22, 2021

Audit End Time:

September 29, 2021

Audited Source Files:

The calculated SHA-256 values for the audited files when the audit was done are as follows:

```
ERC721MinterPauser.sol:
0x9da3da48c3e9afd1ca5aba21635fda7839c580464cfd2d6f2a3aea14816e2e40

ERC721Permit.sol:
0xa716f69b9f68df1df74a48b97052dee86c94de499dd49ec2d63b3d3445522aea

ERC721Royalty.sol:
0xb69263fb32d870c178b5adb62160eb67e755b273aab525fd5c41a17cf78cfb0a

MarketPlaceBase.sol:
0xfee6a0ff9709cad3e5db1454a6da61ccf6718f95be39ffba230e8ae380f1677f

MarketPlaceBid.sol:
0x5985d48407687bb09b1269f6fc2dd283053c9be6e4d03e228f93949beddca838

MarketPlaceListing.sol:
0x1ff39125cb942bf0b95c937c7a1a3b056a94ee511c86c71213fef4059cbfa96d

StartFiMarketPlace.sol:
0xd5cad44e7d4545ee9e9375ef24aa806f6db537a1a55226c50f8cd6b8807a8fd1

StartFiMarketPlaceAdmin.sol:
0xe8cc30799297d6ec40fc90b1bff6d84efd7928a00707ae44ce6b5e2b51173f9d

StartFiMarketPlaceCap.sol:
0xac2f9c03cf83a989e9ce1eb779a54fd775a5528fd72f33b97c3d770184bd2b9e

StartFiMarketPlaceController.sol:
0x905eb9665b81020a2fecb78916c080d04c9cd49ebd8b76594393d6d4547bc3d3
```

```
StartFiMarketPlaceFinance.sol:
0x62b085bc3663e9ce3b4c8dc6005e2c3317f702531321dd8519c3f4ebd5e59451

StartFiMarketPlaceSpecialOffer.sol:
0x732165b8f9080e7c068d8ef12a3eff7484b93df3689ed4c7be24e65b5499f76f

StartFiRoyaltyNFT.sol:
0x742cf5412a7cf684d6fe23ef10673007679bca3579480386ee267d43ba14162f

StartFiToken.sol:
0x8f1c27ec9e3c7298c39fd3813922c17ea98ad6bdcca76e3f411fdbd56c726394

StartFiTokenDistribution.sol:
0x2d5a1cb896b28d5c33d6acb03bd887744b14b8c73be0fcf8e658d46aa26ba834

IERC20.sol:
0xb81b30f92f3efc72d08da2dce6fa5d66e4b6f3e103b6f9902cf967f62b65118f

IERC721Permit.sol:
0x6c908b9ba45176a763e69e1d62af8f518556dcd1a989e2cf3dfbdc352121c518

IERC721Royalty.sol:
0x51d7aa5472632297484123a883b93d1ee0baec6f9f574e09a391df5a9a76bc17

IERC721RoyaltyMinter.sol:
0x8c885fb519accca8292f8277e64273792657986bca67e0128426079cb173926c

IStartFiMarketplace.sol:
0x233cf9816ae8bf8a5e59918aa333e115f994683d7ac3437a2acaf384bb38ed23

IStartFiReputation.sol:
0xa8520ba0ffe96e4a850e354529b668c376fc9693c6f495dda6a3bfe325b44302

IStartFiStakes.sol:
0xb31e095f1fc8c1658c066e4caeeb0d4fcdce15a1b53fd1a43584dce31bbd84e2

SafeDecimalMath.sol:
0x2c4aea23353251259de07cbf03b7701a6459f3447a074dac055771b513a6b850

StartFiFinanceLib.sol:
0x82828956a0a7895efa46f9c9b3c91d8fcfe3be2aa62b8d568bb7638e2fa34ad2

StartFiRoyalityLib.sol:
0xecaeb8aecc08929e35a463093b8b923d8607235317d1e4e16fa508ddba88bce9

StartFiSignatureLib.sol:
0x820592775d439f077fd179d66afa6e0f9991158e882ad4b86f3717fb0fae5afd
```

```
WadRayMath.sol:
0xf3ba269035f300c1aeb5cf7c836b4f30f8516eca11d05423279cef6f3306c833
```

The source files audited include all the files with the extension "sol" as follows:

```
contracts/
├── ERC721MinterPauser.sol
├── ERC721Permit.sol
├── ERC721Royalty.sol
├── MarketPlaceBase.sol
├── MarketPlaceBid.sol
├── MarketPlaceListing.sol
├── StartFiMarketPlace.sol
├── StartFiMarketPlaceAdmin.sol
├── StartFiMarketPlaceCap.sol
├── StartFiMarketPlaceController.sol
├── StartFiMarketPlaceFinance.sol
├── StartFiMarketPlaceSpecialOffer.sol
├── StartFiRoyaltyNFT.sol
├── StartFiToken.sol
├── StartFiTokenDistribution.sol
├── interface
|   ├── IERC20.sol
|   ├── IERC721Permit.sol
|   ├── IERC721Royalty.sol
|   ├── IERC721RoyaltyMinter.sol
|   ├── IStartFiMarketplace.sol
|   ├── IStartFiReputation.sol
|   └── IStartFiStakes.sol
└── library
    ├── SafeDecimalMath.sol
    ├── StartFiFinanceLib.sol
    ├── StartFiRoyalityLib.sol
    ├── StartFiSignatureLib.sol
    └── WadRayMath.sol
```

Note:

- The libraries the contracts rely on were not covered by this audit
- The audit covered the following areas:
  - Startfi Marketplace contract eip-2612 support
  - Startfi ERC721 token with royalty and eip-2612 support
  - Sratfi ERC20 token with eip-2612 support
  - StartFi Token Distribution
- Development of some functions or features are still ongoing. The audited contracts may rely on these functions or features which, we assume, would work as designed and desired.

The goal of this audit is to review StartFi’s solidity implementation for its token issurance and NFT market functions, study potential security vulnerabilities, its general design and architecture, and uncover bugs that could compromise the software in production.

We make observations on specific areas of the code that present concrete problems, as well as general observations that traverse the entire codebase horizontally, which could improve its quality as a whole.

This audit only applies to the specified code, software or any materials supplied by the StartFi team for specified versions. Whenever the code, software, materials, settings, enviroment etc is changed, the comments of this audit will no longer apply.

— Disclaimer

Note that as of the date of publishing, the contents of this report reflect the current understanding of known security patterns and state of the art regarding system security. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk.

The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. If the audited source files are smart contract files, risks or issues introduced by using data feeds from offchain sources are not extended by this review either.

Given the size of the project, the findings detailed here are not to be considered exhaustive, and further testing and audit is recommended after the issues covered are fixed.

To the fullest extent permitted by law, we disclaim all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services.

FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

— The StartFi Team's Consent/Acknowledgement:

The audited materials of the project including but not limited to the documents, home site, source code, etc are all developed, deployed, managed, and maintained outside Mainland CHINA.

The members of the team, the foundation, and all the organizations that participate in the audited project are not Mainland Chinese residents.

The audited project doesn’t provide services or products for Mainland Chinese residents.

— Methodology

The above files' code was studied in detail in order to acquire a clear impression of how the its specifications were implemented. The codebase was then subject to deep analysis and scrutiny, resulting in a series of observations. The problems and their potential solutions are discussed in this document and, whenever possible, we identify common sources for such problems and comment on them as well.

The Fairyproof auditing process follows a routine series of steps:

1. Code review that includes the following
   i. Review of the specifications, sources, and instructions provided to Fairyproof to make sure we understand the size, scope, and functionality of the project's source code.
   ii. Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
   iii. Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to Fairyproof describe.
2. Testing and automated analysis that includes the following:
   i. Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run the test cases.
   ii. Symbolic execution, which is analyzing a program to determine what inputs cause each part of a program to execute.
3. Best practices review, which is a review of the source code to improve maintainability, security, and control based on the established industry and academic practices, recommendations, and research.

— Structure of the document

This report contains a list of issues and comments on all the above source files. Each issue is assigned a severity level based on the potential impact of the issue and recommendations to fix it, if applicable. For ease of navigation, an index by topic and another by severity are both provided at the beginning of the report.

— Documentation

For this audit, we used the following sources of truth about how the StartFi system should work:

http://startf.io/

whitepaper

These were considered the specification, and when discrepancies arose with the actual code behavior, we consulted with the StartFi team or reported an issue.

— Comments from Auditor

No vulnerabilities with critical, high, medium or low-severity were found in the above source code.

Additional notice: 0.

02. About Fairyproof

Fairyproof is a leading technology firm in the blockchain industry, providing consulting and security audits for organizations. Fairyproof has developed industry security standards for designing and deploying blockchain applications.

03. Introduction to StartFi

StartFi is a web3 based multi-channel network for NFT creators.

04. Major functions of audited code

The audited code mainly implements the following functions:

- Issurance of ERC-20 Token
    - Name: to be determined on issurance
    - Symbol: to be determined on issurance
    - Precisions: 18

    - Max Supply: 100,000,000
    - Flexible Max Supply: No
    - Misc:
        - ERC-2612 supported
- Issurance of NFT Tokens
    - Compliant with ERC-721
    - Name: to be determined on issurance
    - Symbol: to be determined on issurance
    - Royalty on NFT: yes
    - Issurance Procedure: to be determined on issurance
    - Misc:
        - ERC-2612 supported
- NFT Market
    - Auction
        - Bidders pay insurance amounts to participate in auctions
        - The winner bidder of an auction needs to pay the winning price within a defined period and then take the auctioned item
        - If the winner bidder doesn't pay the winner price within a defined period, his/her insurance amount will be confiscated.
        - A winner bidder's confiscated insurance amount is sent to both the seller and the platform and each gets 50%.
        - All auctions are English auctions. In a defined auction time, a bidder who offers the highest bid price wins.
        - A seller can set a buyout price for an item such that participants can choose to buy the item.
    - Buyout
    - Transaction Fees
        - The platform charges some fees for an auction
        - There is a royalty for each auctioned item
- Distribution of ERC-20 Tokens
    - Tokens are gradually distributed based on a defined vesting schedule
    - The admin can transfer unlocked tokens

Note:

In an auction when a bidder wins an item and the winning price exceeds a defined value, a KYC is needed before the bidder can fulfill the auction. The KYC is initiated by the admin, therefore an auction may need external centralized operations.

05. Admin rights

In the application the admin has the following previlleges:

- Pausing/resuming the execution of NFT contracts
- Pausing/resuming the execution of NFT market auctions or transactions
- Setting/changing a cap value which is used to trigger a KYC for a seller
- Initiating a KYC for a seller
- Unlocking the insurance amount deposited by a bidder who wins an auction but the seller doesn't go through a KYC. The StartFi team plans to transfer this right to a multi-sig wallet or DAO in the future.
- Setting/changing the transaction fee for a transaction of an NFT item and the address that is used to take insurance amounts
- Setting/changing some core parameters associated with the auction rules and procedures
- Settng/changing the transaction fee's ratio within a range
- Transferring unlocked ERC-20 tokens

06. Key points in audit

During the audit Fairyproof worked closely with the StartFi team and mainly worked on the following items:

- Fixed a bug in the generation of listingIds
- Fixed a bug which might cause a winner bidder to lose his/her insurance amount due to failure of a KYC
- Reduced redundant code
- Refined code implementation in unlocking insurance amounts to reduce gas consumption
- Checked whether or not there were interger overflows/underflows

07. Coverage of issues

The issues that the Fairyproof team covered when conducting the audit include but are not limited to the following ones:

- Re-entrancy Attack
- DDos Attack
- Integer Overflow
- Function Visibility

- Logic Vulnerability
- Uninitialized Storage Pointer
- Arithmetic Precision
- Tx.origin
- Shadow Variable
- Design Vulnerability
- Token Issurance
- Asset Security
- Access Control

08. Severity level reference

Every issue in this report was assigned a severity level from the following:

Critical severity issues need to be fixed as soon as possible.

High severity issues will probably bring problems and should be fixed.

Medium severity issues could potentially bring problems and should eventually be fixed.

Low severity issues are minor details and warnings that can remain unfixed but would be better fixed at some point in the future.

09. List of issues by severity

A. Critical

- N/A

B. High

- N/A

C. Medium

- N/A

D. Low

- N/A

10. List of issues by source file

- N/A

11. Issue descriptions

- N/A

12. Recommendations to enhance the overall security

We list some recommendations in this section. They are not mandatory but will enhance the overall security of the system if they are adopted.

- N/A