Smart Contract Audit Report

Farming-as-a-Service

2023-06-30

BiPOLE Labs
Email: team@bipole.org

CONTENTS

Summary

This report was created for Farming-as-a-Service in order to identify bugs and vulnerabilities in the contract dependencies that were not a part of an officially recognized library as well as project's source code.
Static Analysis and Manual Review approaches have been used to conduct a thorough examination.

The following factors receive extra consideration during the auditing process:
testing the smart contracts for both typical and unusual attack vectors.

* evaluating the codebase to make sure it adheres to the most recent industry standards and best practices.
* ensuring that contract logic adheres to the client's requirements and goals.
* Cross-referencing contract design and execution with related smart contracts created by top industry producers.
* Complete manual line-by-line review of the complete codebase by specialists in the field.

Findings from the security evaluation ranged from important to informative. To guarantee a high degree of security standards and industry practices, we advise taking action on these results. We offer suggestions that, from a security standpoint, could benefit the project.:

* Improve general coding techniques for improved source code organization;
* Include sufficient unit tests to cover all potential use cases.;
* For improved readability, include extra comments for each function, especially for contracts that are publicly verifiable;

* Once the protocol is active, provide additional transparency on privileged operations.

Project Introduction

Farming-as-a-Service allows projects to launch their own farms on the ElkDex using a UI, no code required! These contracts are the most advanced farming contracts in DeFi. They allow builders to reward up to 15 tokens simultaneously. Farm creators can take advantage of Elk's on-chain Impermanent Loss Protection for any given farm and implement any token in the farm as coverage. Elk uses on-chain data with our custom oracle contract, with the necessary security measures, to make sure all farms are protected. The fee to create a farm is quite small, only 1000 ELK (subject to change based on ELK's value). Projects deemed legitimate can be listed on our "Farms" page under the whitelisted section, others can be displayed and are not tagged as whitelisted until they are reviewed.

Audit Scope

ID	Filename	SHA256 CHECK SUM
FIL-1	https://github.com/elkfinance/faas-audit/blob/70d97516db8cce6282dcceaa926210d8a852fd29/contracts/ElkDexOracle.sol	3e9e7805683b75802398dbc7f5c1e853aeb11ef60fb2b35b3336fbb3c1e156a4
FIL-2	https://github.com/elkfinance/faas-audit/blob/70d97516db8cce6282dcceaa926210d8a852fd29/contracts/ElkFactoryHelper.sol	ea8eb0d6aa4594c5c7eee4c6ed96ece67ef913b600d67093f892f2c9c94f4d24
FIL-3	https://github.com/elkfinance/faas-audit/blob/70d97516db8cce6282dcceaa926210d8a852fd29/contracts/ElkFactoryHelperPermissioned.sol	1824b313fd603660a8e29e591b2a06a196c573cb8f2cc4efab2a4787d42d8da4
FIL-4	https://github.com/elkfinance/faas-audit/blob/70d97516db8cce6282dcceaa926210d8a852fd29/contracts/ElkFarmFactory.sol	5b39a9d5789013018850a9cbe57555513be646a5eeae3cdb347dcf3b91afe205
FIL-5	https://github.com/elkfinance/faas-audit/blob/70d97516db8cce6282dcceaa926210d8a852fd29/contracts/FarmManager.sol	cf4c89387a843de08bc18ac55ca9b209cd5198869e3c6c1375efa52316a53adf
FIL-6	https://github.com/elkfinance/faas-audit/blob/70d97516db8cce6282dcceaa926210d8a852fd29/contracts/FarmingRewards.sol	c83087867c7102ba32bf4d671ed9035780efdda561909a133cd4b359fbeec8d2

FIL-7	https://github.com/elkfinance/faas-audit/blob/70d97516db8cce6282dcceaa926210d8a852fd29/contracts/FarmingRewardsPermissoned.sol	ef0d1851dbde8a4ebffdc6b8fbcfc4288fd99592ba6aa62d2387467fac35f955
FIL-8	https://github.com/elkfinance/faas-audit/blob/70d97516db8cce6282dcceaa926210d8a852fd29/contracts/SingleStakeFactory.sol	63c7f5160168ae25d2f5c0c22e51ac56ee19c86a0a7ccb441c8ad5394b7eae62
FIL-9	https://github.com/elkfinance/faas-audit/blob/70d97516db8cce6282dcceaa926210d8a852fd29/contracts/SingleStakeManager.sol	7d9a82addb6254eee22fc95ee844afff456688ad76377ac9027b98c4d67aa0ff
FIL-10	https://github.com/elkfinance/faas-audit/blob/70d97516db8cce6282dcceaa926210d8a852fd29/contracts/SingleStakingRewards.sol	4e0c3566962d3907523591083b225f1dca0d0ef72988b7fe91883307e8679838
FIL-11	https://github.com/elkfinance/faas-audit/blob/70d97516db8cce6282dcceaa926210d8a852fd29/contracts/Staking.sol	ec8180a6b8107a1e834a8d33a8da893219874463e87e5fb55241f1a825a81fd5
FIL-12	https://github.com/elkfinance/faas-audit/blob/70d97516db8cce6282dcceaa926210d8a852fd29/contracts/StakingFee.sol	74eee8513e4c0bc091f5a63bff8d4476c84e387182533ee7a1f388e4fc4f143d
FIL-13	https://github.com/elkfinance/faas-audit/blob/70d97516db8cce6282dcceaa926210d8a852fd29/contracts/StakingRewards.sol	f32bfff0adbbc99c5d758b7209059fdac93d80d4bc7d42d4f2cfe1f8a5913811

Audit Methodology

Step	Operations	Description
1	Backgroud	Reading the descriptions, white papers, contract source code, and other relevant information the project team provides to ensure a proper understanding of project functions.
2	Automated Testing	Automated detection tools will be mainly used to scan the source code to find common potential vulnerabilities
3	Manual Review	The code will be thoroughly reviewed line by line by engineers to find potential vulnerabilities
4	Logic Proofread	The engineer will compare the understanding of the code with the information provided by the project and check whether the code implementation is in line with the white paper information.
5	Test Cases	Including test case design, test scope analysis, symbolic execution, etc.
6	Optimization	Items Review the project from the aspects of maintainability, security and operability according to the application scenarios, call methods and the latest research results.

Risk Levels

Risk Level	Issue Description
Critical	Fatal risks and hazards that need to fixed immediately.
Major	Some high risks and hazards that will lead to related problems that must be solved.
Medium	Some moderate risks and pitfalls may lead to potential risks that will eventually need to be addressed.
Minor	There are low risks and hazards, mainly details of various types of mishandling or warning messages, which can be set aside for the time being.
Informational	Some parts can be optimized, such problems can be shelved, but it is recommended that the final solution.

Vulnerability Summary

ID	Title	Category	Severity	Status
RISK-01	Unchecked update operation	Improvement	Minor	Reported
RISK-02	Unchecked transfer	Improvement	Minor	Fixed
RISK-03	Missing zero address validation	Improvement	Minor	Fixed
RISK-04	External calls inside a loop	Improvement	Minor	Reported
INFO-01	Uses literals with too many digits	Improvement	Information	Fixed
INFO-02	Centralization risk of owner management	Improvement	Information	Fixed
INFO-03	Constant decimal	Improvement	Information	Fixed

RISK-01 | Unchecked update operation

Category	Severity	Location	Status
Improvement	Minor	FIL-1: #121-153	Reported

Description:

The update function being public and allowing unrestricted access to anyone poses a vulnerability in the contract. If someone intentionally utilizes fake or incorrect addresses for _tokenA and _tokenB, it can lead to updating price observations for non-existent or invalid token pairs, resulting in the storage of inaccurate price data.

Recommendation:

Due to hard for recognizing the standard erc20-token onchain, by combining an onlyOwner check and off-chain validation, it can mitigate potential risks associated with invalid or fake token addresses being used in the update function.

RISK-02 | Unchecked transfer

Category	Severity	Location	Status
Improvement	Minor	FIL-4#212; FIL-4#232; FIL-5#225; FIL-11#55; FIL-11#72; FIL-12#110	Fixed

Description:

The return value of an external transfer/transferFrom call is not checked, because several tokens do not revert in case of failure and return false. And also pay attention to honeypot token! In the context of cryptocurrency or decentralized finance (DeFi), the term of honeypot can be used to refer to a smart contract that is intentionally designed to deceive users and trick them into sending funds.

Recommendation:

By checking the return value, you can use SafeERC20, or ensure that the transfer/transferFrom return value is checked, and ensure the desired state changes are successfully executed.

RISK-03 | Missing zero address validation

Category	Severity	Location	Status
Improvement	Minor	FIL-1#85-86	Fixed

Description:

Detect missing zero address validation. If a contract fails to include zero address validation, it can lead to potential vulnerabilities and unexpected behavior, especially without another setting function.

Recommendation:

Check that the address is not zero.

RISK-04 | External calls inside a loop

Category	Severity	Location	Status
Improvement	Minor	FIL-5#226-235; FIL-9#169-178	Reported

Description:

If a function has external calls inside a loop, it can have implications on gas consumption, and potential reentrancy vulnerabilities. And if one of those calls fails to execute properly, it can have implications on the overall behavior and waste of gas consumption.

Recommendation:

Using try-catch can be an effective approach to handle exceptions and errors that may occur during external function calls within a loop.

INFO-01 | Uses literals with too many digits

Category	Severity	Location	Status
Improvement	Information	FIL-4#56; FIL-4#59; FIL-8#44-48	Fixed

Description:

Literals with many digits are difficult to read and review.

Recommendation:

Use Ether suffix, Time suffix or The scientific notation.

INFO-02 | Centralization risk of owner management

Category	Severity	Location	Status
Improvement	Information	FIL-4#240	Fixed

Description:

The overrideOwnership function in the ElkFarmFactory contract is a critical function designed to facilitate the transfer of ownership for farms. It is intended to be used exclusively by the contract owner for security purposes. Due to the use of a single private key, there is a risk of private key loss or private key compromise in extreme cases.

Recommendation:

It is generally recommended that permission control and key contract management functions use multi-signature or timelock for operations, while for functions with centralized servers for automated operations, project parties are required to establish good fault alarm and repair mechanisms to handle unanticipated network conditions in time.

INFO-03 | Constant decimal

Category	Severity	Location	Status
Improvement	Information	FIL-5#137; FIL-5#181	Fixed

Description:

If the token decimal is not 18, such as USDT & USDC, it can affect the accuracy of the calculations in the coverageEarned function. Specifically, the division and multiplication operations involving token balances and coverage values may produce incorrect results.

Recommendation:

Make sure to update all relevant calculations throughout the function to reflect the correct decimal places for the token.

Disclaimer

1 Only the audit types mentioned in the final report published are the subject of this audit report. This audit does not cover any other undiscovered security flaws, and we disclaim all liability for them. ii. A report on an audit may only be based on an attack or vulnerability that existed or had already taken place at the time the report was issued.br/>

2 We are not liable for any new attacks or vulnerabilities that may be launched or arise in the future, and we are unable to predict their likely effects on the security posture of our projects.

3 Prior to the publication of the audit report, the Project Party gave us with certain papers and materials, including but not limited to contract codes, on which we based our security audit analysis and other audit report components. Such documents and materials shall not be false, inaccurate, uninformative, changed, deleted, or concealed, and if the Project Party's documents and materials are false, inaccurate, uninformative, changed, deleted, or concealed, or if the Project Party's documents and materials are untrue, inaccurate, uninformative, altered, deleted, or concealed, or if the Project Party's documents and materials. We shall not be responsible for any loss or negative consequences resulting from any discrepancy between the reflected and actual conditions if the records and information provided by the Project Party are false, inaccurate, uninformative, altered, deleted, or concealed, or if changes are made to such documents and information after the audit report is issued.

4 The Project Parties are aware that our audit report depends on currently available technology and is based on information and documents supplied by the Project Parties. However, there is a chance that our audit report might not fully identify all hazards due to the technical limits of any business. The project development team and any other interested parties are urged to carry out further testing and audits of the project by our audit team.

5 The project owner guarantees that the project is legitimate, compliant, and does not break any laws in the country where the audit or testing is being performed. The audit report is just for the project owner's reference; it should not be used for investment, tax, legal, regulatory, or advisory reasons of any sort, and we will not be held responsible for the contents,

method of acquisition, use, or any services or resources included in the audit report. Without our prior written consent, the Project Party shall not make any references to, quotations from, displays of, or transmissions of the Audit Report, in whole or in part, to any third party. Any damage or liabilities caused by that location is the responsibility of the project party. We disclaim all liability for any reliance or use of the audit report, regardless of its intended use.

6 The compiler of the contract or any other topics outside of the Smart Contract's programming language are not covered in this audit report. The project party is solely responsible for the risk and liability of the audited Smart Contract resulting from references to off-chain data or resources.

About BiPOLE Labs

Through the provision of market-leading smart contract auditing services, BiPOLE Labs, a leading blockchain security company, aims to conduct security and vulnerability research on current blockchain ecosystems. Please contact us for more information at (www.bipole.org) or Email (team@bipole.org)