OVERVIEW

PROJECT SUMMARY

Project	ElevenUp
Platform	Binance Smart Chain
Language	Solidity

AUDIT SUMMARY

Date	30-12-2022
Audit Type	Static Analysis, Manual Review
Audit Result	Pending
Auditor	**Jarmo van de Seijp** https://tinyurl.com/Jvdseijp

RISK SUMMARY

Risk Level	Total	Found	Pending	Solved	Acknowledgde	Objected
Critical	3	3	3	0	0	0
Major	2	2	2	0	0	0
Medium	1	1	1	0	0	0
Minor	3	3	3	0	0	0
Informative	5	5	5	0	0	0
Discussion	0	0	0	0	0	0

FINDINGS

Third party dependency/ unchecked return value

Description:

The contract makes use of the **Aggregator** as a third party service for their price ingestion. The result however, is unchecked. In the case of a faulty return value, the contract may behave in an unexpected way and leave the project's contract with an imprecise state.

Category	Risk Level	Number of Findings	Status
Thrid-Party	Medium	**1**	pending

Lacking zero-check

Description:

The **setExchangeToken** function sets both the price feed and exchange token, but does not check whether these are valid addresses.

Category	Risk Level	Number of Findings	Status
zero-adress	minor	**2**	pending

Expensive Downgrade

Description:

Variable declarations in solidity use a 32-byte memoryslot by default. Using low-bit types like **uint8** for _frozePercentage requires the compiler to downgrade from the standard **uint256** to **uint8**, costing more gas than necessary.

Category	Risk Level	Number of Findings	Status
Gas optimization	Informative	**1**	pending

Unchecked caller ability

Description:

The contract's functions **setNFTAddress** and **setFarmingAddress** set the addresses that are referenced in the **mintAndFreeze** and **mintToFarm** functions as caller of that function. It is worth noting that there is no check as to whether these contract addresses have the ability to call the contract function.

Category	Risk Level	Number of Findings	Status
Unchecked logic	informative	**2**	pending

Lacking contract check

Description:

The addresses set in **setNFTAddress** and **setFarmingAddress** are checked against not being the 0 address, but not against whether or not they are in fact contracts. .

Category	Risk Level	Number of Findings	Status
Unchecked logic	informative	**2**	pending

Incomplete project fulfillment

Description:

The elevenUp token specifies that the **mintAndFreeze** and **mintToFarm** functions are called by the external NFT contract and Farming contract. The deployed contracts, however, don't have the ability to do so.

Category	Risk Level	Number of Findings	Status
Business Logic	Critical	**2**	pending

Push-Over-Pull

Relationship:
CWE-710: Improper Adherence to Coding Standards

Description:

The transfer of the contract's ownership through the function **transferOwnership()** only has 1 check, which is to ensure that the new owner is not the 0 address. It does not, however, check whether or not the ownership can be accepted by the recipient **newOwner**. In the case of a transfer of ownership to an incorrect address, or a smart contract that is not able to use the privileged functions, ownership of the contract is lost permanently with no way of getting it back. It is therefore advisable to use a pull method as opposed to push, in which case the **newOwner** would have to pro-actively accept ownership upon receiving it.

Category	Risk Level	Number of Findings	Status
Push over Pull	Minor	**1**	pending

Incomplete transfer restrictions

Description:

Due to an unmitigated business-logic error, the _frozePercentage and _freezeTime can be circumvented by using the **transferFrom** in stead of the Transfer function.

The token logic checks whether the **msg.sender**'s frozen amount and time is met, which fails to enforce the freezing of tokens since **msg.sender** is the address that interacts with the contract, but not necessarily the address that the tokens are frozen to.

Category	Risk Level	Number of Findings	Status
Business Logic	Critical	**1**	pending

Centralized minting privilege

Description:

The owner can mint an arbitrary amount of tokens to any address without restrictions. This means that the value of the token can potentially be infinitely dilluted in case of compromise of the **owner** account.

Category	Risk Level	Number of Findings	Status
Centralization	Major	**1**	pending

Inconsistent logic

Description:

The **mintToFarm** natspec specifies that the account variable is the _farming address, but fails to enforce this by leaving the account input unchecked.

Category	Risk Level	Number of Findings	Status
Inconsitent Logic	Major	**1**	pending

AUDIT RESULT

Basic Coding Bugs

1. Constructor Mismatch

o Description: Whether the contract name and its constructor are not identical to each other.

o Result: PASSED

o Severity: Critical

Ownership Takeover

o Description: Whether the set owner function is not protected.

o Result: PASSED

o Severity: Critical

Redundant Fallback Function

o Description: Whether the contract has a redundant fallback function.

o Result: PASSED

o Severity: Critical

Overflows & Underflows

Description: Whether the contract has general overflow or underflow Vulnerabilities

o Result: PASSED

o Severity: Critical

Reentrancy

o Description: Reentrancy is an issue when code can call back into your contract and change state, such as withdrawing ETHs.

o Result: PASSED

o Severity: Critical

MONEY-Giving Bug

o Description: Whether the contract returns funds to an arbitrary address.

o Result: PASSED

o Severity: High

Blackhole

- *Description: Whether the contract locks ETH indefinitely: merely in without out.*
- *Result: PASSED*
- *Severity: High*

Unauthorized Self-Destruct

- *Description: Whether the contract can be killed by any arbitrary address.*
- *Result: PASSED*
- *Severity: Medium*

Revert DoS

- *Description: Whether the contractis vulnerable to DoSattack because of unexpected revert.*
- *Result: PASSED*
- *Severity: Medium*

Unchecked External Call

- *Description: Whether the contract has any external call without checking the return value.*
- *Result: PASSED*
- *Severity: Medium*

Gasless Send

- *Description: Whether the contractis vulnerable to gasless send.*
- *Result: PASSED*
- *Severity: Medium*

Send Instead of Transfer

- *Description: Whether the contract uses send instead of transfer.*
- *Result: PASSED*
- *Severity: Medium*

Costly Loop

o Description: Whether the contract has any costly loop which may lead to Out-Of-Gas exception.

o Result: PASSED

o Severity: Medium

(Unsafe) Use of Untrusted Libraries

o Description: Whether the contract use any suspicious libraries.

o Result: PASSED

o Severity: Medium

(Unsafe) Use of Predictable Variables

o Description: Whether the contract contains any randomness variable, but its value can be predicated.

o Result: PASSED

o Severity: Medium

Transaction Ordering Dependence

o Description: Whether the final state of the contract depends on the order of the transactions.

o Result: PASSED

o Severity: Medium

. Deprecated Uses

o Description: Whether the contract use the deprecated tx.origin to perform the authorization.

o Result: PASSED

o Severity: Medium