OVERVIEW

PROJECT SUMMARY

Project	**ARULSINGAM (ARSI)**
Platform	N/a
Language	Solidity

AUDIT SUMMARY

Date	01-03-2022
Audit Type	Static Analysis, Manual Review
Audit Result	**Passed**
Auditor	**Jarmo van de Seijp** https://tinyurl.com/Jvdseijp

RISK SUMMARY

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

FINDINGS

Unused Code

SWC-ID: SWC-101

Relationship:
CWE-710: Improper Adherence to Coding Standards

Description:
Functions that do not have a function visibility type specified are public by default. This can lead to a vulnerability if a developer forgot to set the visibility and a malicious user is able to make unauthorized or unintended state changes.

Relevance:
The openZeppeling erc20 standard uses default function visibility of public where this may not be needed. To avoid issues with 3rd party applications, it's the accepted practise to leave the erc20 interface functions defined as public in stead of 'external'

Category	Risk Level	Number of Findings	Status
SWC-101	Informative	**5**	Acknowledged

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