AUDIT.SC

Smart Contract Audit

BRING TRUST IN YOUR PROJECT

AUDIT-SC
PARTNER
AVACASH

WWW.AUDIT.SC

2022

FULL SMART CONTRACT AUDIT

SOLIDITY CHECK

Audit SC Guarantees that every smart contract that has been audited has gone through both automated Smart Contract Scanner Softwares and is manually verified by one of our highly experienced smart contract experts.

Table of Contents

AUDIT-SC

DISCLAIMER

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and AUDIT-SC and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (AUDIT-SC) owe no duty of care towards you or any other person, nor does AUDIT-SC make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided «as is», without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and AUDIT-SC hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, AUDIT-SC hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against AUDIT-SC, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

OVERVIEW

PROJECT SUMMARY

Project	**https://github.com/avacash/avacash-contracts-core/tree/79600794075f0c769f18ac43b35ea5df5d60b4b8/contracts**
Platform	Avalanche
Language	Solidity

AUDIT SUMMARY

Date	07-02-2022
Audit Type	Static Analysis, Manual Review
Audit Result	**Passed**

RISK SUMMARY

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

FINDINGS

Unused Code

SWC-ID: SWC-131

Relationship:
CWE-1164: Irrelevant Code

Description:
Unused variables are allowed in Solidity and they do not pose a direct security issue. It is best practice though to avoid them as they can: cause an increase in computations (and unnecessary gas consumption) indicate bugs or malformed data structures and they are generally a sign of poor code quality cause code noise and decrease readability

Relevance:
Both this and the below issue relate to the unlocked variable

Category	Risk Level	Number of Findings	Status
SWC-131	Informative	**1**	Solved

Constable State

SWC-ID: SWC-101

Relevance:
Labeling the visibility explicitly makes it easier to catch incorrect assumptions about who can access the variable.

Category	Risk Level	Number of Findings	Status
SWC-108	Informative	**1**	Solved

FINDINGS

Unused Code

SWC-ID: SWC-131

Relationship:
CWE-1164: Irrelevant Code

Description:
Unused variables are allowed in Solidity and they do not pose a direct security issue. It is best practice though to avoid them as they can: cause an increase in computations (and unnecessary gas consumption) indicate bugs or malformed data structures and they are generally a sign of poor code quality cause code noise and decrease readability

Relevance:
SafeMathUni.div is not used and can be removed

Note from Auditor:
"
As it is convention to implement libraries with their entire code base, this point may be ignored. Though, the project being a financial ecosystem, it's worth noting that the dead code (from a safe library) is adding is gas cost.
"

The client has acknowledged that the safeMath library is only partially used in the smart contract functions. Though, due to the unit testing relying on its existing and it posing no threat whatsoever, decided to keep the original safeMath library unchanged.

Category	Risk Level	Number of Findings	Status
SWC-131	Discussion	**1**	Acknowledged

Missing Event

Description:
The function flashLoan depends on the value of flashloanFee for calculations. The change of this variable is not emitted as an event. This may cause 3rd party applications as well as users to miss the change in fee on taking flashloans, potentially causing unwanted outcome for users or aggregators

Category	Risk Level	Number of Findings	Status
Missing-events	Medium	**1**	Solved

FINDINGS

Lack of checking Zero-Address in Constructor

Description:
The constructor sets (address _flashLoanFeeReceiver), but does not check if the address is the zero address. When deploying multiple instances of this smart contract automatically, this may be accidentally the case.

Category	Risk Level	Number of Findings	Status
Lacking Checks	Minor	**1**	Solved

Typo's / Spelling errors

Description:
The contract uses words like "Thru" (#92 and #104) as opposed to "Through", and "Payed" in stead of "Paid" (#99). This is, of course, not a vulnerability but might be misconstrued as lacking attention to detail by observers or users of the contract

Category	Risk Level	Number of Findings	Status
Informational	informational	**3**	Solved

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

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

Unauthorized Self-Destruct

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

Revert DoS

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

Unchecked External Call

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

Gasless Send

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

Send Instead of Transfer

- o Description: Whether the contract uses send instead of transfer.
- o Result: PASSED
- o 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

AUDIT.SC

CONTACT US

Audit SC Guarantees that every smart contract that has been audited has gone through both automated Smart Contract Scanner Softwares and is manually verified by

E-mail: info@audit.sc

Website: www.audit.sc

AUDIT.SC