ASTROBIATECH
BLOCKCHAIN SECURITY

MADE IN INDIA
BLOCKCHAIN SECURITY

SECURITY ASSESSMENT REPORT

PREPARED FOR

AquawaUSDT

@astrobiatech

Nov
2023

astrobiatech.in

TABLE OF CONTENTS

SCOPE OF AUDIT

The scope of this audit was to analyze and document the AquawaUSDT smart contract codebase for quality, security, and correctness.

CHECKED VULNERABILITIES

We have scanned the smart contract for commonly known and morespecific vulnerabilities. Here are some of the commonly known vulnerabilities that we considered:

- Re-entrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Use of tx.origin
- Exception disorder
- Gasless send
- Balance equality
- Byte array
- Transfer forwards all gas
- ERC20 API violation
- Malicious libraries
- Compiler version not fixed
- Redundant fallback function
- Send instead of transfer
- Style guide violation
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level

TECHNIQUES & METHODS

Throughout the audit of smart contract, care was taken to ensure:

- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behaviour.
- Token distribution and calculations are as per the intended behaviour mentioned in the whitepaper.
- Implementation of ERC-20 token standards.
- Efficient use of gas.
- Code is safe from re-entrancy and other vulnerabilities.

The following techniques, methods and tools were used to review all thesmart contracts.

Static Analysis

Static Analysis of Smart Contracts was done to identify contract vulnerabilities. In this step a series of automated tools are used to testsecurity of smart contracts.

Code Review / Manual Analysis

Manual Analysis or review of code was done to identify new vulnerability or verify the vulnerabilities found during the static analysis.Contracts were completely manually analyzed, their logic was checkedand compared with the one described in the whitepaper. Besides, the results of automated analysis were manually verified.

ISSUE CATEGORIES

Every issue in this report has been assigned with a severity level. There are four levels of severity and each of them has been explained below.

➢ HIGH SEVERITY ISSUES

A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality and we recommend these issues to be fixed before movingto a live environment.

➢ MEDIUM SEVERITY ISSUES

The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems and they should still be fixed.

➢ LOW SEVERITY ISSUES

Low level severity issues can cause minor impact and or are just warningsthat can remain unfixed for now. It would be better to fix these issues atsome point in the future.

➢ INFORMATIONAL

These are severity four issues which indicate an improvement request, ageneral question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

ISSUES TABLE

TYPE	HIGH	MEDIUM	LOW	INFORMATIONAL
OPEN	2	0	0	0
ACKNOWLWDGENT	-	-	-	-
CLOSED	2	-	-	-

INTRODUCTION

On 23-11-2023 – Astrobiatech Blockchain Security Team performed security audit for AquawaUSDT smart contract.

CONTRACT NAME	AquawaUSDT
CONTRACT ADDRESS	0x53FD3c7dfDa8e91161e5De72253C0C001bB8fd1E
BLOCKCHAIN	Binance Smart Chain

OVERVIEW

CONTRACT ADDRESS
0x53FD3c7dfDa8e91161e5De72253C0C001bB8fd1E

CONTRACT NAME
AquawaUSDT

CONTRACT CREATOR
0xC9ad4B019a0C7247eB9F12161aDE28940CaD8797

OWNER ADDRESS
0xC22424cf2677D76958497E75B2aB11e4a6CCbF0c

SOURCE CODE
Contract Source Code Verified at Binance Smart Chain

OTHER SETTINGS
default evmVersion, MIT license

COMPILER VERSION
v0.8.0+commit.c7dfd78e

OPTIMIZATION ENABLED
Yes with 200 runs

Code is truncated to fit the constraints of this document.
https://bscscan.com/address/0x53fd3c7dfda8e91161e5de72253c0c001bb8fd1e#code

MANUAL ANALYSIS FINDINGS

HIGH

1. Referral Bonus Levels and Potential Impact on USDT Balances

Description:-

Once user reach the referrals count criteria, they will receive the corresponding bonus for this level on each new referral. This can drain contract's current usdt balances if bonuses are too high.

Recommendation:-

Users should not receive referrals count reward more than once for each level.

Referral's rewards value should not exceed the minimum deposit multiplied by referrals count criteria.

2. 180-Day Stake Trigger Prevention

Description:-

Stake for 180 days will never trigger, because if the user is new they will be marked as 'old' user in the lines above push stake logic.

Recommendation:-

User's status should be changed after pushing the new Stake.

AUTOMATED ANALYSIS

```
INFO:Detectors:
 AquawaUSDT.calculateEarnings(uint256,uint256) (token.sol#296-302) performs a multiplication on the result
of a division:
        - earningsPercentage = timeDiff * dailyInterestRate / 86400 (token.sol#298)
        - earnings = amount * earningsPercentage / 100 (token.sol#299)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
AquawaUSDT.stake(uint256,address).reward (token.sol#175) is a local variable never initialized
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#uninitialized-local-variables
```

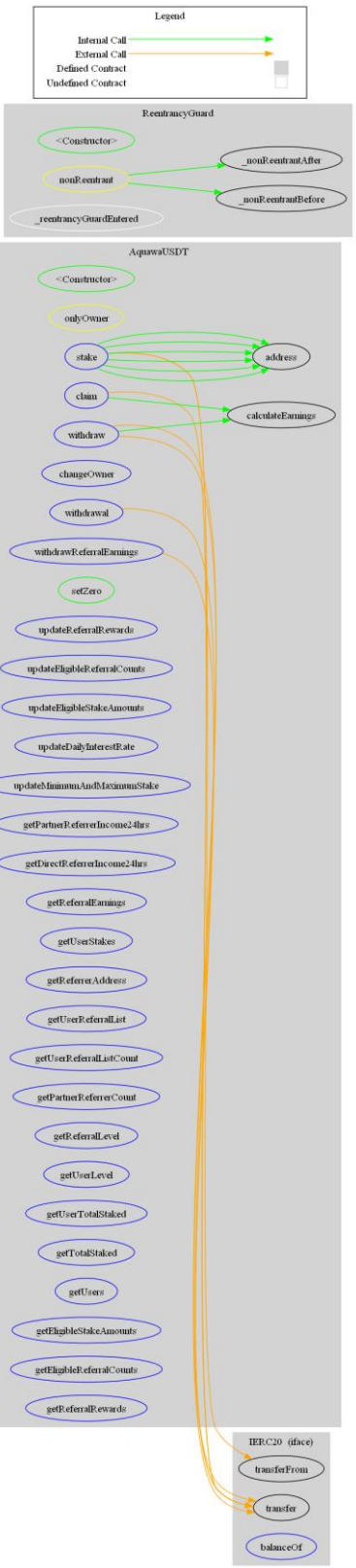
FUNCTIONAL ANALYSIS

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
AquawaUSDT	Implementation	ReentrancyGuard		
└	<Constructor>	Public !	🛑	NO !
└	stake	External !	🛑	nonReentrant
└	claim	External !	🛑	nonReentrant
└	withdraw	External !	🛑	nonReentrant
└	calculateEarnings	Public !		NO !
└	changeOwner	External !	🛑	onlyOwner
└	withdrawal	External !	🛑	onlyOwner
└	withdrawReferralEarnings	External !	🛑	nonReentrant
└	setZero	Public !	🛑	onlyOwner
└	updateReferralRewards	External !	🛑	onlyOwner nonReentrant
└	updateEligibleReferralCounts	External !	🛑	onlyOwner nonReentrant
└	updateEligibleStakeAmounts	External !	🛑	onlyOwner nonReentrant
└	updateDailyInterestRate	External !	🛑	onlyOwner nonReentrant
└	updateMinimumAndMaximumStake	External !	🛑	onlyOwner nonReentrant
└	getPartnerReferrerIncome24hrs	External !		NO !
└	getDirectReferrerIncome24hrs	External !		NO !
└	getReferralEarnings	External !		NO !
└	getUserStakes	External !		NO !
└	getReferrerAddress	External !		NO !
└	getUserReferralList	External !		NO !
└	getUserReferralListCount	External !		NO !
└	getPartnerReferrerCount	External !		NO !
└	getReferralLevel	External !		NO !
└	getUserLevel	External !		NO !
└	getUserTotalStaked	External !		NO !
└	getTotalStaked	External !		NO !
└	getUsers	External !		NO !
└	getEligibleStakeAmounts	External !		NO !
└	getEligibleReferralCounts	External !		NO !
└	getReferralRewards	External !		NO !

Legend

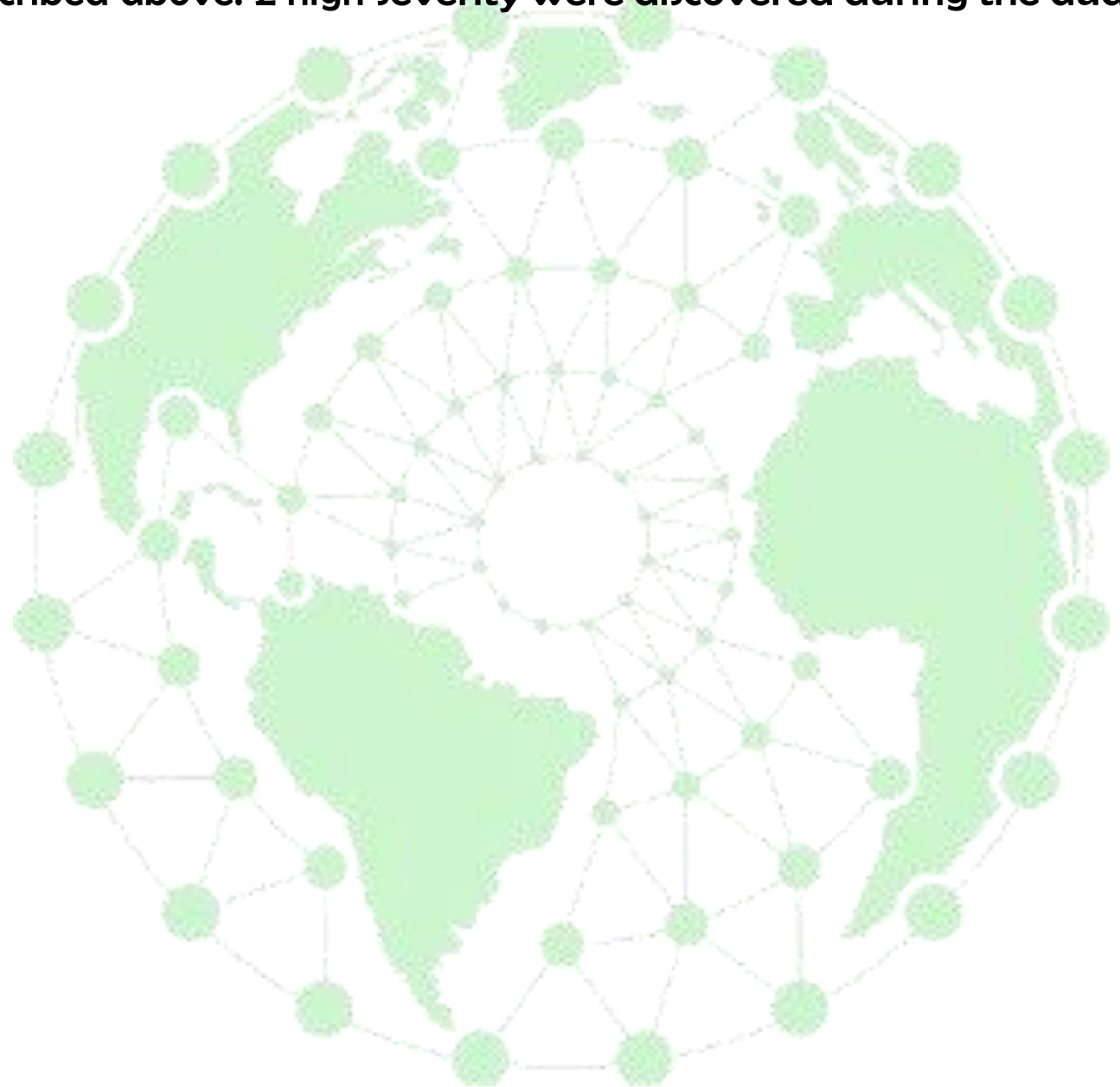
Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

GRAPH TREE



SUMMARY

In this report, we have considered the security of the AquawaUSDT smart contract. We performed our audit according to the procedure described above. 2 high severity were discovered during the audit.



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 constituteinvestment advice. No one shall have any right to rely on the report or its contents, and Astrobiatech Blockchain Security and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Astrobiatech BlockchainSecurity) owe no duty of care towards you or any other person, nor does Astrobiatech Blockchain Security 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 Astrobiatech Blockchain Security 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 effectin relation to the report. Except and only to the extent that it is prohibited by law, Astrobiatech Blockchain Security hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Astrobiatech Blockchain Security, 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 lossor 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. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Proofed by Astrobiatech

ASTROBIATECH
BLOCKCHAIN SECURITY

https://astrobiatech.in

@astrobiatech