KAIZEN GLOBAL

Title

Blockchain Security

Smart Contract
Final Audit Report

KaizenGlobal.org

contact@KaizenGlobal.org

+92 334 0738638

info@thekaizenglobal.co

S-19 Second Floor, Gold Mall
Murree Road Rawalpindi

Contents

1. Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice 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 disclaimer below – please make sure to read it in full.

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 KaizenGlobal and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives) (KaizenGlobal) owe no duty of care towards you or any other person, nor does KaizenGlobal make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "asis", without any conditions, warranties, or other terms of any kind except as set out in this disclaimer, and KaizenGlobal 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. Exceptand only to the extent that it is prohibited by law, KaizenGlobal hereby excludes all liability and responsibility,and neither you nor any other person shall have any claim against KaizenGlobal, 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 the 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. KaizenGlobal owns all copyright rights to the text, images, photographs, and other content provided in the following document. When using or sharing partly or in full, third parties must provide a direct link to the original document mentioning the author (thekaizenglobal.com).

2. Overview

KaizenGlobal was commissioned by the BLU Token team to perform an audit of their smart contract.The audit was conducted between 31/05/2023 and 01/06/2023.

The purpose of this audit was to achieve the following:

- Identify potential security issues with smart contracts
- Formally check the logic behind given smart contracts.

Information in this report should be used for understanding the risk exposure of smart contracts, and as a guide to improving the security posture of smart contracts by remediating the issues that were identified.

The code is available at Binanace Smart Chain:

BLU Token 0x6B7c184fE5D316D9a26E3C5dE5a2c91b4EE03022.

2.1 Summary

Project name	BLU
Platform	Binanace Smart Chain

Language	Solidity

2.2 Contracts

Name	Address
ERC20BSC.sol	0x6B7c184fE5D316D9a26E3C5dE5a2c91b4EE03022

3. Found issues

High	0 (0%)
Medium	0 (0%)
Low	3 (100%)
Info	0 (0%)

C1. ERC20BSC.sol

ID	Severity	Title	Status
C1-03	Low	Fixed Compiler Version	Acknowledged
C1-04	Low	Ownership Issue	Acknowledged
C1-05	Low	withdrawERC20FromContract checks	Acknowledged

4. Contracts

C1. ERC20BSC.sol

Overview

This token is using basic implementation of the OpenZeppline ERC20 and Ownable standard. It's also using OpenZeppline SafeErc20 interface to transfer other token's that are transferred to this contract address.

Issues

C1-01 Issue# 1 — Low — Acknowledged

Fixed Compiler Version

Recommendation

It's preferred you should use a fixed

Compiler Version Example:

Current: pragma solidity ^0.8.17;
Updated: pragma solidity 0.8.17;

C1-02 Issue# 2 — Low — Acknowledged

Ownership issue

Recommendation

If you are deploying the contract yourself it would be better you don't pass the owner in the constructor. If you don't pass it deployer will be the owner.

C1-03 Issue# 3 — Low — Acknowledged

withdrawERC20FromContract checks

Recommendation

In the withdrawERC20FromContract function there should be a check that _to address can't be address zero and _amount transfer shouldn't be zero

Conclusion

The reviewed contract doesn’t have any major issues.

Appendix A. Issues' severity classification

- **Critical.** Issues that may cause an unlimited loss of funds or entirely break the contract workflow. Malicious code (including malicious modification of libraries) is also treated as a critical severity issue. These issues must be fixed before deployments or fixed in already running projects as soon as possible.
- **High.** Issues that may lead to a limited loss of funds, break interaction with users, or other contracts under specific conditions. Also, issues in a smart contract, that allow a privileged account the ability to steal or block other users' funds.
- **Medium.** Issues that do not lead to a loss of funds directly, but break the contract logic. May lead to failures in contracts operation.
- **Low.** Issues that are of a non-optimal code character, for instance, gas optimization tips, unused variables, errors in messages.
- **Informational.** Issues that do not impact the contract operation. Usually, informational severity issues are related to code best practices, e.g. style guide.

Appendix B. List of examined issue types

- Business logic overview
- Functionality checks
- Following best practices
- Access control and authorization
- Reentrancy attacks
- Front-run attacks
- DoS with (unexpected) revert
- DoS with block gas limit
- Transaction-ordering dependence
- ERC/BEP and other standards violation
- Unchecked math
- Implicit visibility levels
- Excessive gas usage
- Timestamp dependence
- Forcibly sending ether to a contract
- Weak sources of randomness
- Shadowing state variables
- Usage of deprecated code

KAIZEN GLOBAL

Kaizen Global

Blockchain Security

+92 334 0738638

info@thekaizenglobal.co

S-19 Second Floor, Gold Mall
Murree Road Rawalpindi