CERTIK

CertiK Audit Report for DUCATO

Contents

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Verification Services Agreement between CertiK and DUCATO (the "Company"), or the scope of services/verification, and terms and conditions provided to the Company in connection with the verification (collectively, the "Agreement"). This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without CertiK's prior written consent.

About CertiK

CertiK is a technology-led blockchain security company founded by Computer Science professors from Yale University and Columbia University built to prove the security and correctness of smart contracts and blockchain protocols.

CertiK, in partnership with grants from IBM and the Ethereum Foundation, CertiK's mission of every audit is to apply different approaches and detection methods, ranging from manual, static, and dynamic analysis, to ensure that projects are checked against known attacks and potential vulnerabilities. CertiK leverages a team of seasoned engineers and security auditors to apply testing methodologies and assessments to each project, in turn creating a more secure and robust software system.

CertiK has served more than 100 clients with high quality auditing and consulting services, ranging from stablecoins such as Binance's BGBP and Paxos Gold to decentralized oracles such as Band Protocol and Tellor. CertiK customizes its engineering tool kits, while applying cutting-edge research on smart contracts, for each client on its project to offer a high quality deliverable. For more information: https://certik.io.

Executive Summary

This report has been prepared for **DUCATO** to discover issues and vulnerabilities in the source code of their **DUCATO ERC-20 Smart Contract** as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Dynamic Analysis, Static Analysis, and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Testing Summary

SECURITY LEVEL

TBD

Smart Contract Audit

This report has been prepared as a product of the Smart Contract Audit request by DUCATO.

This audit was conducted to discover issues and vulnerabilities in the source code of the DUCATO ERC-20 Smart Contract.

TYPE	Smart Contract
SOURCE CODE	https://etherscan.io/address/0xa117ea1c0c85cef648df2b6f40e50bb5475c228d#code
PLATFORM	EVM
LANGUAGE	Solidity
REQUEST DATE	July 31, 2020
DELIVERY DATE	Aug 03, 2020
METHODS	A comprehensive examination has been performed using Dynamic Analysis, Static Analysis, and Manual Review.

Review Notes

Introduction

CertiK team was contracted by the DUCATO team to audit the design and implementation of their token smart contract and its compliance with the EIPs it is meant to implement.

The audited source code link is:

- Token Source Code: https://etherscan.io/address/0xa117ea1c0c85cef648df2b6f40e50bb5475c228d#code

The goal of this audit was to review the Solidity implementation for its business model, study potential security vulnerabilities, its general design and architecture, and uncover bugs that could compromise the software in production.

The findings of the initial audit have been conveyed to the team behind the contract implementations and the source code is expected to be re-evaluated before another round of auditing has been carried out.

Documentation

The sources of truth regarding the operation of the contracts in scope were minimal although the token fulfilled a simple use case we were able to fully assimilate. To help aid our understanding of each contract's functionality we referred to in-line comments and naming conventions.

These were considered the specification, and when discrepancies arose with the actual code behaviour, we consulted with the DUCATO team or reported an issue.

Summary

The codebase of the project is a typical EIP20 implementation with additional support for a full transfer freezing mechanism and an approve-and-call mechanism for interacting with other contracts.

Certain optimization steps that we pinpointed in the source code mostly referred to coding standards and inefficiencies and no vulnerabilities or attack vectors were identified during our audit.

The codebase of the project strictly adheres to the standards and interfaces imposed by the OpenZeppelin open-source libraries and as such its typical ERC-20 functions **can be deemed to be of high security and quality, however the custom functionality built on top of it possessed flaws** we identified.

Recommendations

Overall, the codebase of the contracts should be refactored to assimilate the findings of this report, enforce linters and / or coding styles as well as correct any spelling errors and mistakes that appear throughout the code **to achieve a high standard of code quality and security**.

Findings

Exhibit 1

TITLE	TYPE	SEVERITY	LOCATION
Unlocked Compiler Version	Language Specific	Informational	All “pragma” statements

[INFORMATIONAL] Description:

The smart contract “pragma” statements regarding the compiler version indicate that version 0.5.0 or higher should be utilized.

Recommendations:

We advise that the compiler version is locked at version 0.5.0 or whichever Solidity version higher than that satisfies the requirements of the codebase as an unlocked compiler version can lead to discrepancies between compilations of the same source code due to compiler bugs and differences.

Exhibit 2

TITLE	TYPE	SEVERITY	LOCATION
Mutability Specifiers Missing	Language Specific	Informational	DUCATO: L95, L96, L97, L98

[INFORMATIONAL] Description:

The aforementioned lines contain contract level declarations that are assigned to only once during the construction of the contract with literal values.

Recommendations:

As the assignments are literal values, it is possible to set these variables to “constant” variables that contain the value they are assigned with directly and thus optimize any utilization of the variables within the codebase.

Exhibit 3

TITLE	TYPE	SEVERITY	LOCATION
Visibility Specifiers Missing	Language Specific	Informational	DUCATO: L98, L99, L101, L102

[INFORMATIONAL] Description:

The aforementioned lines contain contract level declarations that do not specify their visibility via one of the corresponding keywords.

Recommendations:

We advise that a strict visibility specifier is set for these variables to aid in the legibility of the codebase.

Exhibit 4

TITLE	TYPE	SEVERITY	LOCATION
Redundant Subtraction	Mathematical	Informational	DUCATO: L123

[INFORMATIONAL] Description:

The aforementioned line subtracts the balance of the zero address from the total supply before returning it, hinting that the address acts as a burn mechanism.

Recommendations:

As all contract functions prohibit the transfer of tokens to the zero address, the burn mechanism is never in place and thus the balance of the zero address will always be zero. We advise that this subtraction is removed and that the total supply variable is instead properly renamed and set to “public”.

Exhibit 5

TITLE	TYPE	SEVERITY	LOCATION
Unconventional Greater-Than Comparisons	Logical	Informational	DUCATO: L160, L197, L198

[INFORMATIONAL] Description:

The aforementioned comparisons conduct a greater-than “>” comparison between the dynamic variable and the address of zero to prevent from transmitting funds to and out of it.

Recommendations:

These comparisons should instead be changed to inequalities as addresses are meant to be strictly compared rather than numerically compared.