Security Assessment

Kaizen.Finance

Sept 15th, 2021

Table of Contents

Summary

This report has been prepared for Kaizen to discover issues and vulnerabilities in the source code of the Kaizen.Finance project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing 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.

Additionally, this audit is based on a premise that all external smart contracts are safely implemented.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	Kaizen.Finance
Platform	Ethereum
Language	Solidity
Codebase	https://github.com/KaizenFinance/CollateralizedToken
Commit	aba38db65963656bf0bf368de68775b1be01d779

Audit Summary

Delivery Date	Sept 15, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
Major	1	0	0	1	0	0
Medium	1	0	0	1	0	0
Minor	0	0	0	0	0	0
Informational	1	0	0	1	0	0
Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
CTK	CollateralizedToken.sol	a4964364b3522d3eef2c50ef441ee98ead16e0733513a9bc36a543088e5cef53
ERC	ERC20TokenImplementationOriginal.sol	8fc0b0f033465e3ea1399fa8b5f119dd682423f1cff5a8fecd520be8be9eec2f

Understandings

Overview

The `VestingToken` contract of KaiZen Finance is a project that helps users to launch a vesting schedule on the blockchain. A vesting schedule is about gradually unlocking a certain amount of tokens to recipients during a certain period.

`vesting` token is the certificate that recipients hold to swap the `original token` that is allocated to recipients. `vesting` token balance of any user/address contains the following two states: `Unlocked balance`, the amount of the vesting tokens that may already be swapped to original tokens; `Locked balance`, the amount of the vesting tokens that may not yet be swapped to original tokens. The exchange ratio between vesting tokens and original tokens is 1:1. External users deposit `original token` into `VestingToken` as collateral and airdrop `vesting` token to recipients by calling the `airdrop()` function. And the `Admin` can transfer unused collateral in `original token` to a specified address.

The vesting timeline contains three key time points, `TGE(Token Generation Event)`, `startTickTimestamp`, and `endTickTimestamp`. The `block.timestamp` is used to determine whether or not the aforementioned key timepoint is reached. In the beginning, all minted `vesting` tokens are locked in the `VestingToken` contract. At `TGE`, the `tgePercentage` amount, whose value is set during the initialization step, of one user's `vesting` token while it is being unlocked. There is nothing that happens in the `cliffDuration` between `TGE` and `startTickTimestamp`. After `TGE`, all remaining locked `vesting` tokens would be gradually unlocked in the duration between `startTickTimestamp` and `endTickTimestamp`. That duration is equally divided into multiple periods, each period is called `tick`. The minimal acceptable `tick` period is 60 seconds. In each `tick` , the formula `lockedVestingToken * [(currentTick - lastUpdateTick) / (lastTick - lastUpdateTick)]` is used to calculate how many locked `vesting` tokens would be unlocked. If the `lastTick` is reached, the all-locked `vesting` token is unlocked. Recipients can use the unlocked `vesting` tokens to swap the original token.

Users also can transfer their holding `vesting` token, which is locked or unlocked, by calling the `customTransfer()` function or `ERC20` standard transfer methods.

Privileged Functions

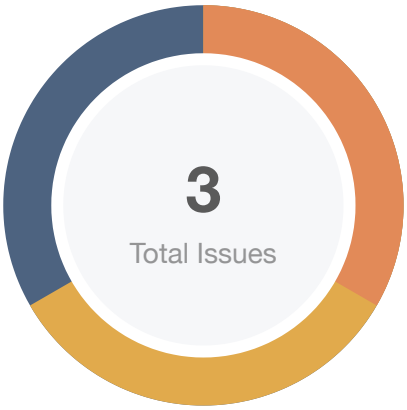
The contract contains the following privileged functions that are restricted by the `onlyAdmin` modifier. They are used to modify the contract configurations and address attributes. We group these functions below:

The `onlyAdmin` modifier:

- `setTgeTimestamp()` in `CollateralizedToken.sol`

- `withdrawUnusedCollateral()` in `CollateralizedToken.sol`

Findings



Critical	**0** (0.00%)
Major	**1** (33.33%)
Medium	**1** (33.33%)
Minor	**0** (0.00%)
Informational	**1** (33.33%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
CTK-01	Privileged Ownership	**Centralization / Privilege**	**Major**	Acknowledged
CTK-02	Missing Input Validation	Volatile Code	Informational	Acknowledged
ERC-01	Token Minted To Designated Address	Control Flow	Medium	Acknowledged

CTK-01 | Privileged Ownership

Category	Severity	Location	Status
Centralization / Privilege	**Major**	CollateralizedToken.sol: 905, 912	Acknowledged

Description

The role `admin` has the authority over the listed functions. Any compromise to the `admin` account may allow a potential hacker to take advantage of this and execute malicious acts.

- `setTgeTimestamp()` in `CollateralizedToken.sol`
- `withdrawUnusedCollateral()` in `CollateralizedToken.sol`

Recommendation

We advise the client to carefully manage the role `admin` account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

Indicatively, here are some feasible suggestions that would also mitigate the potential risk at the different levels in terms of short-term and long-term scenarios:

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

The response from the client is as below:

Sure, we are aware of these facts, applicable to the whole crypto industry. Would recommend users using multisig wallets and automate their creation in the future.

CTK-02 | Missing Input Validation

Category	Severity	Location	Status
Volatile Code	Informational	CollateralizedToken.sol: 787~791	Acknowledged

Description

The given input is missing the check for `_tgeTimestamp` validation.

Recommendation

We advise adding the check for the passed-in values to prevent unexpected errors as below:

```
787  function setTgeTimestamp(Vesting storage _self, uint256 _tgeTimestamp) internal
onlyBeforeTge(_self) {
788      require(_tgeTimestamp >= block.timestamp, "CollateralizedToken: _tgeTimestamp is
before current block timestamp");
789
790      _self.tgeTimestamp = _tgeTimestamp;
791
792      emit SetTgeTimestamp(_tgeTimestamp);
793  }
```

Alleviation

The response from the client is as below:

It's done to let token owners initiate TGE timestamp even after TGE because the team is always busy on TGE day and may forget to set it up.

ERC-01 | Token Minted To Designated Address

Category	Severity	Location	Status
Control Flow	Medium	ERC20TokenImplementationOriginal.sol: 223	Acknowledged

Description

The function `initialize()` will be called to sets all of the initial states for the contract. According to its logic, `totalSupply` tokens will be mint to `recipient`.

Recommendation

Please ensure the accuracy of `recipient` when calling this function. We also advise the client to adopt Multisig, Timelock, and/or DAO in the project to manage this address.

Alleviation

The response from the client is as below:

We specially added the “recipient” entity to let issuer mint tokens to the secure destination that may be MultiSig, DAOs, or others. We would provide users with the one-click multisig wallet creation tool for this process and inform them about the importance of security of token destination (recipient).

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

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 Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with 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, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS

AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING

MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.