CERTIK

Security Assessment

Trusttoken #2

Sept 13th, 2021

Table of Contents

Summary

This report has been prepared for Trust Token to discover issues and vulnerabilities in the source code of the Trusttoken #2 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.

The codebase of the project is very well coded with proper commenting and design. It respects for the most part the language best practices and idioms.

Overview

Project Summary

Project Name	Trusttoken #2
Description	Credit System
Platform	Ethereum
Language	Solidity
Codebase	https://github.com/trusttoken/smart-contracts
Commit	d6f31eb8d8a92f2cf6302de31ebd16b7a563d319

Audit Summary

Delivery Date	Sept 13, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

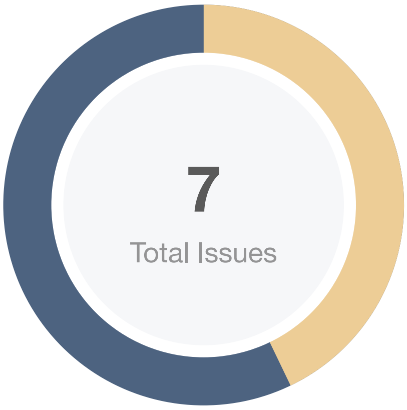
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
● Critical	0	0	0	0	0	0
● Major	0	0	0	0	0	0
● Medium	0	0	0	0	0	0
● Minor	3	0	0	0	0	3
● Informational	4	0	0	0	0	4
● Discussion	0	0	0	0	0	0

Audit Scope

ID	Repo	Commit	File	SHA256 Checksum
LFN	trusttoken/smart-contracts	d6f31eb	truefi2/LoanFactory3.sol	c36500ea860e380b2e2043031783e9400c1351cb70d84dd1073fda28a415f6fe
SBR	trusttoken/smart-contracts	d6f31eb	truefi2/SpotBaseRateOracle.sol	1cea23800d7e4a883256583c47e2174da479658e2bc537a846c5fa1e6a0216ef
TAB	trusttoken/smart-contracts	d6f31eb	truefi2/TimeAveragedBaseRateOracle.sol	e78103872f21d4d92b2569be2a70f28dc80f4ef53c758e41bbf14feab530c8b2
TCA	trusttoken/smart-contracts	d6f31eb	truefi2/TrueCreditAgency.sol	d7493e3c3bcaa373619a2ed1421f327086e72277671c4a2b5a14820b8a728eba
TFC	trusttoken/smart-contracts	d6f31eb	truefi2/TrueFiCreditOracle.sol	fc31b44832a39fc50d184eb24ac4f834bb70e9c51ac52a9c9ffce03bd26008c8
TRA	trusttoken/smart-contracts	d6f31eb	truefi2/TrueRateAdjuster.sol	12e474f2f7a3cd8c6299b2153f37863b8a7eca6a477d06130c7b7b718f96a18d

Findings



🟥 **Critical**	**0** (0.00%)
🟧 **Major**	**0** (0.00%)
🟨 **Medium**	**0** (0.00%)
🟨 **Minor**	**3** (42.86%)
🟦 **Informational**	**4** (57.14%)
🟩 **Discussion**	**0** (0.00%)

ID	Title	Category	Severity	Status
LFN-02	Ambiguous Functionality	Logical Issue	● Informational	✓ Resolved
LFN-03	Missing Zero Address Check	Logical Issue	● Minor	✓ Resolved
SBR-01	Variable Declare as Immutable	Gas Optimization	● Minor	✓ Resolved
TCA-01	Redundant Variable Initialization	Coding Style	● Informational	✓ Resolved
TCA-04	Inefficient Casting	Gas Optimization	● Informational	✓ Resolved
TFC-01	Missing Zero Address Check	Logical Issue	● Minor	✓ Resolved
TRA-01	Hardcoded Value Could Be A Constant	Coding Style	● Informational	✓ Resolved

LFN-02 | Ambiguous Functionality

Category	Severity	Location	Status
Logical Issue	● Informational	truefi2/LoanFactory3.sol: 80~82	✓ Resolved

Description

The linked function describes a external that sets the admin to a hard coded address.

Recommendation

Consider adding a rationale regarding the given functionality.

Alleviation

The team has fixed the issue in commit up to 1f1ee7c970b57cfea8d8e3c75404ed17b78efaa7.

LFN-03 | Missing Zero Address Check

Category	Severity	Location	Status
Logical Issue	● Minor	truefi2/LoanFactory3.sol: 117~120	✓ Resolved

Description

The linked code does not check against a zero address case.

Recommendation

Consider implementing a check against a zero address case.

Alleviation

The team has fixed the issue in commit up to 1f1ee7c970b57cfea8d8e3c75404ed17b78efaa7.

SBR-01 | Variable Declare as Immutable

Category	Severity	Location	Status
Gas Optimization	● Minor	truefi2/SpotBaseRateOracle.sol: 15	✓ Resolved

Description

The variable aaveLendingPool assigned in the constructor can be declared with `Immutable`. Immutable state variables can be assigned during contract creation but will remain constant throughout the lifetime of a deployed contract. A big advantage of immutable variables is that reading them is significantly cheaper than reading from regular state variables since will not be stored in storage. Still, values will directly insert the values into the runtime code.

Recommendation

We recommend using an immutable state variable for aaveLendingPool.

Alleviation

The team has fixed the issue in commit up to 1f1ee7c970b57cfea8d8e3c75404ed17b78efaa7.

TCA-01 | Redundant Variable Initialization

Category	Severity	Location	Status
Coding Style	● Informational	truefi2/TrueCreditAgency.sol: 256, 275	✓ Resolved

Description

All variable types within Solidity are initialized to their default ""empty"" value, which is usually their zeroed out representation.

Particularly:

- `uint` / `int`: All `uint` and `int` variable types are initialized at `0`
- `address`: All `address` types are initialized to `address(0)`
- `byte`: All `byte` types are initialized to their `byte(0)` representation
- `bool`: All `bool` types are initialized to `false`
- `ContractType`: All contract types (i.e. for a given `contract ERC20 {}` its contract type is `ERC20`) are initialized to their zeroed out address (i.e. for a given `contract ERC20 {}` its default value is `ERC20(address(0))`)
- `struct`: All `struct` types are initialized with all their members zeroed out according to this table

Recommendation

We advise that the linked initialization statements are removed from the codebase to increase legibility.

Alleviation

The team has fixed the issue in commit up to 1f1ee7c970b57cfea8d8e3c75404ed17b78efaa7.

TCA-04 | Inefficient Casting

Category	Severity	Location	Status
Gas Optimization	● Informational	truefi2/TrueCreditAgency.sol: 260	✓ Resolved

Description

The linked code declares a uint8 variable instead of a uint256.

Recommendation

Consider using uint256 instead of uint8 as local variables are not packed.

Alleviation

The team has fixed the issue in commit up to 1f1ee7c970b57cfea8d8e3c75404ed17b78efaa7.

TFC-01 | Missing Zero Address Check

Category	Severity	Location	Status
Logical Issue	● Minor	truefi2/TrueFiCreditOracle.sol: 133~136	✓ Resolved

Description

The linked code does not check against a zero address case.

Recommendation

Consider implementing a check against a zero address case.

Alleviation

The team has fixed the issue in commit up to 1f1ee7c970b57cfea8d8e3c75404ed17b78efaa7.

TRA-01 | Hardcoded Value Could Be A Constant

Category	Severity	Location	Status
Coding Style	● Informational	truefi2/TrueRateAdjuster.sol: 335~338	✓ Resolved

Description

The linked code contains a hardcoded value that is repeated.

Recommendation

Consider introducing a constant to represent the value.

Alleviation

The team has fixed the issue in commit up to 1f1ee7c970b57cfea8d8e3c75404ed17b78efaa7.

Appendix

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.

CERTIK