CERTIK

Security Assessment

# Camell

CertiK Assessed on May 10th, 2024

CertiK Assessed on May 10th, 2024

# Camell

The security assessment was prepared by CertiK, the leader in Web3.0 security.

## Executive Summary

| TYPES | ECOSYSTEM | METHODS |
|---|---|---|
| TRC-20 | Tron (TRX) | Formal Verification, Manual Review, Static Analysis |

| LANGUAGE | TIMELINE | KEY COMPONENTS |
|---|---|---|
| Solidity | Delivered on 05/10/2024 | N/A |

CODEBASE
https://tronscan.io/#/token20/TTLVdtBYipLVqVbPaaQb2Zbcubbpddtxu7/code
View All in Codebase Page

COMMITS
TTLVdtBYipLVqVbPaaQb2Zbcubbpddtxu7
View All in Codebase Page

## Vulnerability Summary

| 5 | 0 | 0 | 0 | 5 | 0 |
|---|---|---|---|---|---|
| Total Findings | Resolved | Mitigated | Partially Resolved | Acknowledged | Declined |

| | | | |
|---|---|---|---|
| 0 | Critical | | Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks. |
| 2 | Major | 2 Acknowledged | Major risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project. |
| 0 | Medium | | Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform. |
| 0 | Minor | | Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions. |
| 3 | Informational | 3 Acknowledged | Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code. |

# TABLE OF CONTENTS | CAMELL

# CODEBASE | CAMELL

## Repository

https://tronscan.io/#/token20/TTLVdtBYipLVqVbPaaQb2Zbcubbpddtxu7/code

## Commit

TTLVdtBYipLVqVbPaaQb2Zbcubbpddtxu7

# AUDIT SCOPE | CAMELL

5 files audited ● 3 files with Acknowledged findings ● 2 files without findings

| ID | Repo | File | SHA256 Checksum |
|---|---|---|---|
| MRC | CertiKProject/certik-audit-projects | contarcts/MinterRole.sol | 9cf84936cc0c50d249ed70b6d4bdd4d5e5a1c5c703b6beb26f237487eb63a4a6 |
| TRC | CertiKProject/certik-audit-projects | contarcts/TRC20.sol | 3894a0e62fd5fec2bbce20e6d3b00e91b670074439079e2eec7a053a6938142c |
| TRM | CertiKProject/certik-audit-projects | contarcts/TRC20Mintable.sol | 299a1969984ebb97bd7cb770b8404a2fdef36bb946adc328ff9e71c81cccaae1 |
| TRB | CertiKProject/certik-audit-projects | contarcts/TRC20Burnable.sol | 26655b6788d4504303534ea6af6cb42d640608075271a4c83f4ea2ed5a2ac1de |
| ITR | CertiKProject/certik-audit-projects | contarcts/ITRC20.sol | 1ec3e47f74ae6b0bb6bec9d615b29b615b1aeaad0c4980c4773febb78c58b56a |

# APPROACH & METHODS | CAMELL

This report has been prepared for Camell to discover issues and vulnerabilities in the source code of the Camell project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Formal Verification, Manual Review, and Static Analysis 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 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:

- Testing the smart contracts against both common and uncommon attack vectors;
- 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.

# REVIEW NOTES | CAMELL

## Overview

**CAMT** is a standard `TRC20` token that is deployed on the **Tron** chain.

## Privileged Functions

In the **Camell** project, several roles are adopted to operate with some of the key functionalities of the implemented contract. Such privileged roles and methods are described in the findings:

- **TRC-01: Initial Token Distribution**
- **CKP-01: Centralization Risks**

The advantage of this privileged role in the codebase is that the client reserves the ability to adjust the protocol according to the runtime required to best serve the community. It is also worth of note the potential drawbacks of these functions, which should be clearly stated through the client's action/plan. Additionally, if the private key of the privileged account is compromised, it could lead to devastating consequences for the project.

To improve the trustworthiness of the project, dynamic runtime updates in the project should be notified to the community. Any plan to invoke the aforementioned functions should be also considered to move to the execution queue of the `Timelock` contract.

# FINDINGS | CAMELL

| 5 | 0 | 2 | 0 | 0 | 3 |
|---|---|---|---|---|---|
| Total Findings | Critical | Major | Medium | Minor | Informational |

This report has been prepared to discover issues and vulnerabilities for Camell. Through this audit, we have uncovered 5 issues ranging from different severity levels. Utilizing the techniques of Formal Verification, Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

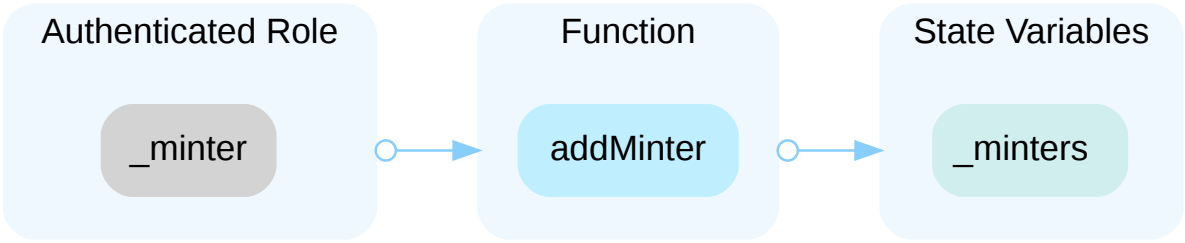
| ID | Title | Category | Severity | Status |
|---|---|---|---|---|
| **CKP-01** | **Centralization Risks** | **Centralization** | **Major** | **Acknowledged** |
| **TRC-01** | **Initial Token Distribution** | **Centralization** | **Major** | **Acknowledged** |
| MRC-01 | Missing Emit Events | Coding Style | Informational | Acknowledged |
| TRC-02 | Too Many Digits | Coding Style | Informational | Acknowledged |
| TRC-03 | Meaningless Type Convert | Logical Issue | Informational | Acknowledged |

# CKP-01 | CENTRALIZATION RISKS

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Centralization | Major | contarcts/MinterRole.sol: 16; contarcts/TRC20Mintable.sol: 10 | Acknowledged |

## Description

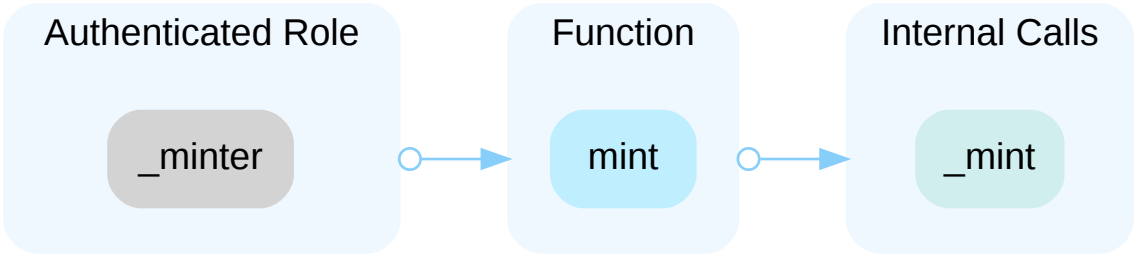
In the contract `MinterRole` the role `_minter` has authority over the functions shown in the diagram below.




Any compromise to the `_minter` account may allow the hacker to take advantage of this authority and add malicious accounts to the minter list.

---

In the contract `TRC20Mintable` the role `_minter` has authority over the functions shown in the diagram below.




Any compromise to the `_minter` account may allow the hacker to take advantage of this authority and manipulate users' balances.

## Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol 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 a different level in terms of short-term, long-term and permanent:

### Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND
- A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

### Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.
  AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

### Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles.
  OR
- Remove the risky functionality.

## Alleviation

**[Camell Team,05/10/2024]**:
Issue acknowledged. I won't make any changes for the current version.

**[CertiK,05/10/2024]**:
As the minter roles can mint tokens at will, CertiK strongly encourages the project team periodically revisit the private key security management of all minter accounts.

# TRC-01 | INITIAL TOKEN DISTRIBUTION

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| **Centralization** | **Major** | **contarcts/TRC20.sol: 17** | **Acknowledged** |

## Description

All of the **CAMT** tokens are sent to the contract deployer or one or several externally-owned account (EOA) addresses. This is a centralization risk because the deployer or the owner(s) of the EOAs can distribute tokens without obtaining the consensus of the community. Any compromise to these addresses may allow a hacker to steal and sell tokens on the market, resulting in severe damage to the project.

## Recommendation

It is recommended that the team be transparent regarding the initial token distribution process. The token distribution plan should be published in a public location that the community can access. The team should make efforts to restrict access to the private keys of the deployer account or EOAs. A multi-signature (⅔, ⅗) wallet can be used to prevent a single point of failure due to a private key compromise. Additionally, the team can lock up a portion of tokens, release them with a vesting schedule for long-term success, and deanonymize the project team with a third-party KYC provider to create greater accountability.

## Alleviation

**[Camell Team,05/10/2024]**:
Issue acknowledged. I won't make any changes for the current version.

**[CertiK,05/10/2024]**:
As compromise to these addresses may allow a hacker to steal and sell tokens on the market, resulting in severe damage to the project, CertiK strongly encourages the project team periodically revisit the private key security management of all these accounts.

# MRC-01 | MISSING EMIT EVENTS

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Coding Style | Informational | contarcts/MinterRole.sol: 16, 20 | Acknowledged |

## Description

Functions that update sensitive state variables should emit relevant events as notifications.

## Recommendation

Recommend adding events for state-changing actions, and emitting them in their relevant functions.

## Alleviation

**[Camell Team,05/10/2024]**:

Issue acknowledged.

# TRC-02 | TOO MANY DIGITS

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Coding Style | Informational | contarcts/TRC20.sol: 16 | Acknowledged |

## Description

Literals with many digits are difficult to read and review.

## Recommendation

Recommend using scientific notation (e.g. `1e6`) or underscores (e.g. `1_000_000`) to improve readability.

## Alleviation

**[Camell Team,05/10/2024]**:

Issue acknowledged.

# TRC-03 | MEANINGLESS TYPE CONVERT

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Logical Issue | Informational | contarcts/TRC20.sol: 16 | Acknowledged |

## Description

Converting `decimals` to uint256 is not required.

## Recommendation

Recommend using `decimals` directly.

## Alleviation

**[Camell Team,05/10/2024]**:

Issue acknowledged.

# APPENDIX | CAMELL

## Finding Categories

| Categories | Description |
| --- | --- |
| Coding Style | Coding Style findings may not affect code behavior, but indicate areas where coding practices can be improved to make the code more understandable and maintainable. |
| Logical Issue | Logical Issue findings indicate general implementation issues related to the program logic. |
| Centralization | Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code. |

## 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 | CERTIK

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.

# CertiK | Securing the Web3 World

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.