CERTIK

Security Assessment

The Legend of Deification

Sept 8th, 2021

Table of Contents

Summary

This report has been prepared for The Legend of Deification to discover issues and vulnerabilities in the source code of the The Legend of Deification 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 implemented safely.

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	The Legend of Deification
Platform	Ethereum
Language	Solidity
Codebase	https://github.com/BWNFT/Legend-NFT
Commit	79ebad4cf1cb664a3268cfbf9bcd14292449d81b 1e7455cb2da55b1c1fdf781510e8f5647f81dae3

Audit Summary

Delivery Date	Sept 08, 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	2	0	0	1	0	1
Minor	0	0	0	0	0	0
Informational	1	0	0	0	0	1
Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
ATL	Auth.sol	c2f912ede3b59e6f805b66dac8410f5d8f77af27dbbf8408d1940af6c571ef91
CAR	CARD.sol	170528742cc475701ca3a9e3aaa83e97ed9d829e0bcb3c0df44da1114e61f248
ERC	ERC721.sol	88769222342a25637ce3ba053067927863eb3a2a551bfb5086e5494deae75796
ERT	ERC721Token.sol	42fca16971367503463df07343ccd332bf95cec77c6e25df4b2aa45cf48b9a1d
PAC	PACK.sol	7933d139337becae28c4d9c2b6fcadc1197585e2e895bcdb840128382dd6e8aa
SKI	SKILL.sol	4b52446eabc594e353b34a079e3d8015fb253b4f258d691095f7d3e3d7379cdf
TLO	TLOD.sol	886987bc39d46e57cefa1e35893b74185b197f6f859313f580d5f985679f1f69

Understandings

Overview

The Legend of Deification is an NFT project based on `ERC721 Non-Fungible Token Standard.` CARD`,` PACK`, and` SKILL`contracts are inherited from the`ERC721Token `contract which is inherited from the`ERC721` contract.

The `Auth` contract is responsible for access restriction. There are three different kinds of roles , `address(this)`, `_owner`, and `_authority`, can be authorized to access sensitive functions, such as `mint()`, `safeMint`, `burn()`, etc.

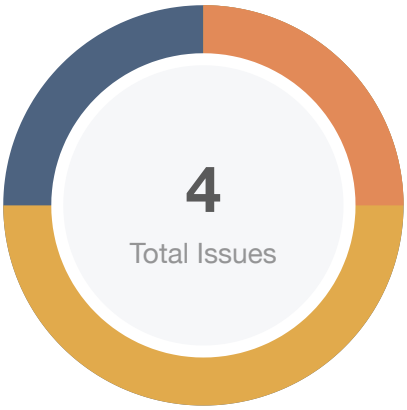
`TLOD` is an `ERC20` contract that mints the `_totalSupply` amount of token to a centralized address when it is deployed onto blockchain.

Privileged Functions

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

- `setOwner()` in `Auth.sol`
- `setAuthority()` in `Auth.sol`
- `setBaseURI()` in `ERC721Token.sol`
- `setTokenURI()` in `ERC721Token.sol`
- `mint()` in `ERC721Token.sol`
- `safeMint(address to, uint256 tokenId)` in `ERC721Token.sol`
- `safeMint(address to,uint256 tokenId,bytes memory _data)` in `ERC721Token.sol`
- `burn()` in `ERC721Token.sol`

Findings



Critical	**0** (0.00%)
Major	**1** (25.00%)
Medium	**2** (50.00%)
Minor	**0** (0.00%)
Informational	**1** (25.00%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
GLOBAL-01	Unlocked Compiler Version	Language Specific	Informational	Resolved
GLOBAL-02	Centralization Risk	**Centralization / Privilege**	**Major**	Acknowledged
ATL-01	Missing Input Validation	Volatile Code	Medium	Resolved
TLO-01	Token Minted To Centralized Address	Logical Issue	Medium	Acknowledged

GLOBAL-01 | Unlocked Compiler Version

Category	Severity	Location	Status
Language Specific	Informational	Global	Resolved

Description

The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

Recommendation

We advise that the compiler version is alternatively locked at the lowest version possible that the contract can be compiled at. For example, for version `v0.8.0` the contract should contain the following line:

```
pragma solidity 0.8.0;
```

Alleviation

The development team resolved this issue in commit 1e7455cb2da55b1c1fdf781510e8f5647f81dae3.

GLOBAL-02 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	**Major**	**Global**	Acknowledged

Description

The role `owner` has the authority over the the following functions:

- `setOwner()` in `Auth.sol`
- `setAuthority()` in `Auth.sol`
- `setBaseURI()` in `ERC721Token.sol`
- `setTokenURI()` in `ERC721Token.sol`
- `mint()` in `ERC721Token.sol`
- `safeMint(address to, uint256 tokenId)` in `ERC721Token.sol`
- `safeMint(address to,uint256 tokenId,bytes memory _data)` in `ERC721Token.sol`
- `burn()` in `ERC721Token.sol`

Any compromise to the `owner` account may allow a potential hacker to take advantage of this and execute malicious acts.

Recommendation

We advise the client to carefully manage the role `owner` 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 client responded that they would use the recommended and their own methods to protect the private key of the `owner`.

ATL-01 | Missing Input Validation

Category	Severity	Location	Status
Volatile Code	Medium	new_version/Auth.sol: 28~31, 33~36	Resolved

Description

The given input is missing the check for non-zero address.

Recommendation

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

```
28 function setOwner(address owner) external onlyAuth {
29     require(address(0) != owner, "set owner to the zero address");
30     _owner = owner;
31     emit SetOwner(_owner);
32 }
```

```
33 function setAuthority(address authority) external onlyAuth {
34     require(address(0) != owner, "set authority to the zero address");
35     _authority = authority;
36     emit SetAuthority(_authority);
37 }
```

Alleviation

The development team resolved this issue in commit 1e7455cb2da55b1c1fdf781510e8f5647f81dae3.

TLO-01 | Token Minted To Centralized Address

Category	Severity	Location	Status
Logical Issue	Medium	new_version/TLOD.sol: 19	Acknowledged

Description

The `_totalSupply` amount of token is minted to a centralized address. This may raise community concerns about the centralized issue.

Recommendation

We advise the client to carefully manage the `ERC20` deployer account's private key and avoid any potential risks of being hacked. We also advise the client to adopt Multisig, Timelock, and/or DAO in the project to manage this specific account in this case.

Alleviation

The client responded that the tokens, which are minted when the contract is deployed, would be transferred to the address of the `Game Operation Department`. And the client would use the recommended and their own methods to protect the private key of the `ERC20` deployer account.

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.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

Volatile Code

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

Language Specific

Language Specific findings are issues that would only arise within Solidity, i.e. incorrect usage of private or delete.

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.