CERTIK

Preliminary Comments

Illuvium Land Sale Protocol

May 13th, 2022

Table of Contents

Summary

Overview

- Project Summary
- Audit Summary
- Vulnerability Summary
- Audit Scope

Findings

- IGB-01 : Lack of Input Validation
- IGB-02 : Requisite Value of ERC-20 `transferFrom()` / `transfer()` Call
- IGB-03 : Missing Error Messages
- IGT-01 : Missing Emit Events
- LSI-01 : Centralization Related Risks
- LSI-02 : `_pauseDuration` Incorrectly Emitted
- LSP-01 : Hardcoded Oracle Answer Update Timeframe

Appendix

Disclaimer

About

Summary

This report has been prepared for Landsale to discover issues and vulnerabilities in the source code of the Illuvium Land Sale Protocol 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 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	Illuvium Land Sale Protocol
Platform	Ethereum
Language	Solidity
Codebase	https://github.com/IlluviumGame/land-sale-core
Commit	b331088ab710142b9776c053268303b7f189c1a4

Audit Summary

Delivery Date	May 13, 2022 UTC
Audit Methodology	Static Analysis, Manual Review

Vulnerability Summary

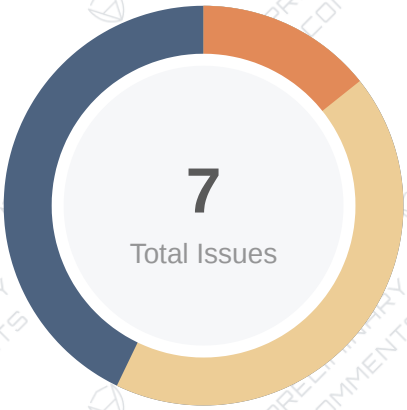
Vulnerability Level	Total	Pending	Declined	Acknowledged	Mitigated	Partially Resolved	Resolved
Critical	0	0	0	0	0	0	0
Major	1	0	0	1	0	0	0
Medium	0	0	0	0	0	0	0
Minor	3	0	0	1	0	0	2
Informational	3	0	0	0	0	1	2
Discussion	0	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
LSL	contracts/lib/LandSvgLib.sol	54cfd190738df3a10133a7168d62c6fa5e0a3da45d5e423f944afbcb71556915
ACI	contracts/utils/AccessControl.sol	79d1bef7dabe60a72b67d6c8865d3bd812c417f9d6629773386567b87b99e396
ERE	contracts/interfaces/ERC721SpecExt.sol	049587f274a3d53d35a115ee22d5d2c4a4d2e3050e456078421ce0d4f315fed9
LER	contracts/interfaces/LandERC721Spec.sol	781247e832e3e794b17580e3ce8640e455958eaaf1c3835a9528d5533995a6e5
ISG	contracts/interfaces/ImmutableSpec.sol	1aa1801d70c574322238c797a2e965e437d0922718e8cd9cfe46743941c9afa5
ERS	contracts/interfaces/ERC20Spec.sol	0697479909b8e127e2da1f60f3a8fea10ff975802c287a078b949beda3fba68b
LLI	contracts/lib/LandLib.sol	682eb85d05154e47e64ddf71c1b14ed0cc1eb4ee38d65abe2b41951384e1b1a1
LBL	contracts/lib/LandBlobLib.sol	66c7465e72d08e0e9e72f7e94cacf1efc4e69bc3149399133995b6906722ed76
ERG	contracts/token/ERC20Impl.sol	b71376843aba9209d8213723b152f3a92f049e386567249c57042537431433f1
UER	contracts/token/UpgradeableERC721.sol	a9c174dc25631a2843bf4bcefdefc10680946e8f95a79e2e4904fd5dbb84f9f9
LSI	contracts/protocol/LandSale.sol	077589850227829 4f2c8617f1cad00823607071 00de93146dd77c1d581bf30b7
LDI	contracts/token/LandDescriptorImpl.sol	13c3c53a2c4067875e8d8db56428f47b113b4307d802fc07ed46ed8cfebbb2c4
ECI	contracts/token/ERC721Impl.sol	2b1c59cb18460524741b3c4dc6004e89a98928202770050e4a9b3e1b537583c8
LEC	contracts/token/LandERC721.sol	d2b137bac8cd4816c05ecf0c02dc1982336c32ae3764fd0176fcb7e7a03ca67d
ERC	contracts/interfaces/ERC165Spec.sol	c2b5c217e1130dc8dce304dde924ef52dde4c31a8a2be3e01f658ef4e2547fd6
RER	contracts/token/RoyalERC721.sol	dc3f068ed0a9576da9a5f5471313bce459312e1dae5a03b0a7c2732a5fdd837b

ID	File	SHA256 Checksum
ERI	contracts/interfaces/ERC721Spec.sol	ec4dff135822086a9b4584194425f80359d0082bd9c1ac31b5ec6ef01ca9a2b4
EIP	contracts/interfaces/EIP2981Spec.sol	20f08c667cf60e02956eef5c108fa76bccc058d53f7c50d5e23a5698cae99443
POS	contracts/interfaces/PriceOracleSpec.sol	d551550eb2120d070f4b39785b1fd5c6a06d8765d9886bfb0a42ae17394d06e3
ISI	contracts/interfaces/IdentifiableSpec.sol	057e7616143e59190337cd4f856292a7dfe0e9531d3f6e5cebd12b3c84d37dda
UAC	contracts/utils/UpgradeableAccessControl.sol	28b6e16cfb07169b54ade92977b9a50799a23506f9513c6505362030db2f0085
LSP	contracts/protocol/LandSalePriceOracleV1.sol	5b404b1ec9c743c56ec7ac936d43c0dfc031188687227c915276e2faac865cf7

Findings



Critical	0 (0.00%)
Major	1 (14.29%)
Medium	0 (0.00%)
Minor	3 (42.86%)
Informational	3 (42.86%)
Discussion	0 (0.00%)

ID	Title	Category	Severity	Status
IGB-01	Lack Of Input Validation	Volatile Code	Minor	Acknowledged
IGB-02	Requisite Value Of ERC-20 `transferFrom()` / `transfer()` Call	Logical Issue	Minor	Resolved
IGB-03	Missing Error Messages	Coding Style	Informational	Resolved
IGT-01	Missing Emit Events	Coding Style	Informational	Partially Resolved
LSI-01	Centralization Related Risks	**Centralization / Privilege**	**Major**	Acknowledged
LSI-02	`_pauseDuration` Incorrectly Emitted	Logical Issue	Informational	Resolved
LSP-01	Hardcoded Oracle Answer Update Timeframe	Coding Style	Minor	Resolved

IGB-01 | Lack Of Input Validation

Category	Severity	Location	Status
Volatile Code	Minor	contracts/token/LandERC721.sol: 38, 46, 285; contracts/lib/LandLib.sol: 200	Acknowledged

Description

in `setMetadata()`, there are no input validations on `Site Type` and `Landmark Type ID`, where

- `Site Type` must be in the range of [1, 6]
- `Landmark Type ID` must be in the range of [0, 7]

Recommendation

Consider adding the require() checks for `Site Type` and `Landmark Type ID` in `setMetadata()`

Alleviation

`[Illuvium]`:

1.Site Type is not part of the setMetadata() input(s) Landmark Type ID can be potentially any number.

2. Current version of the game recognizes only values in range [0,7] which is enforced by LandSale contract. Same applies to the regionId, coordinates, etc.

Please clarify your suggestion. What piece of documentation is confusing and requires clarification?

`[CertiK]`: In the function `setMetadata()`, the input `_plot` comes with the `Internal Land Structure` data according to the comments at L31 to L54, in which the `Type ID` and `Landmark Type ID` are explicitly defined in enumerating way. In this case, there should be validation check to guarantee the input value of `Type ID` and `Landmark Type ID` in `_plot` are valid in the function `setMetadata()`

IGB-02 | Requisite Value Of ERC-20 `transferFrom()` / `transfer()` Call

Category	Severity	Location	Status
Logical Issue	Minor	contracts/interfaces/ERC20Spec.sol: 107, 132; contracts/protocol/LandSale.sol: 1; contracts/token/ERC721Impl.sol: 1; contracts/token/UpgradeableERC721.sol: 1	Resolved

Description

While the ERC-20 implementation does necessitate that the `transferFrom()` / `transfer()` function returns a `bool` variable yielding `true`, many token implementations do not return anything i.e. Tether (USDT) leading to unexpected halts in code execution.

Recommendation

We advise that the `SafeERC20.sol` library is utilized by OpenZeppelin to ensure that the `transferFrom()` / `transfer()` function is safely invoked in all circumstances.

Alleviation

`[CertiK]`: The team heeded the advice and merged the change into the master. Final commit hash to be provided by the team after all the issues are fixed and merged.

IGB-03 | Missing Error Messages

Category	Severity	Location	Status
Coding Style	Informational	contracts/protocol/LandSale.sol: 480, 481; contracts/mocks/ChainlinkAggregatorV3Mock.sol: 102	Resolved

Description

The **require** can be used to check for conditions and throw an exception if the condition is not met. It is better to provide a string message containing details about the error that will be passed back to the caller.

Recommendation

We advise adding error messages to the linked **require** statements.

Alleviation

`[CertiK]`: The team heeded the advice and merged the change into the master. Final commit hash to be provided by the team after all the issues are fixed and merged.

IGT-01 | Missing Emit Events

Category	Severity	Location	Status
Coding Style	Informational	contracts/token/UpgradeableERC721.sol: 321, 348; contracts/token/ERC20Impl.sol: 117, 158; contracts/token/ERC721Impl.sol: 306, 333	Partially Resolved

Description

There should always be events emitted in the sensitive functions that are controlled by centralization roles.

Recommendation

It is recommended emitting events for the sensitive functions that are controlled by centralization roles.

Alleviation

`[Illuvium]`: Issue refers to mint/burn events in the ERC20/ERC721 contracts.

These functions always emit a standard Transfer event. Please clarify your recommendation. Do you suggest emitting also another type of event which would include the address which executed the restricted operation?

`[CertiK]`: A specific emitting event for each specific type of operation/function is recommended for transaction logging

LSI-01 | Centralization Related Risks

Category	Severity	Location	Status
Centralization / Privilege	**Major**	contracts/protocol/LandSale.sol: 1	Acknowledged

Description

In the contract `LandSale.sol`, the following roles has authority over the following functions:

- `ROLE_DATA_MANAGER` role has authority over function `setInputDataRoot()`
- `ROLE_SALE_MANAGER` role has authority over function `initialize()`
- `ROLE_PAUSE_MANAGER` role has authority over function `pause()`
- `ROLE_PAUSE_MANAGER` role has authority over function `resume()`
- `ROLE_WITHDRAWAL_MANAGER` role has authority over function `setBeneficiary()`
- `ROLE_WITHDRAWAL_MANAGER` role has authority over function `withdrawTo()`
- `ROLE_RESCUE_MANAGER` role has authority over function `rescueErc20()`
-

Any compromise to the privileged roles may allow a hacker to take advantage of this authority and update the sensitive settings and execute sensitive functions of the project.

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., multi-signature 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.

Noted: Recommend considering the long-term solution or the permanent solution. The project team shall make a decision based on the current state of their project, timeline, and project resources.

Alleviation

`[Illuvium]`: Current deployment process implies transferring all the roles to Illuvium eDAO mSig wallet (4/6 signatures) It also implies that any permissions which are no longer required to extend, or/and upgrade the protocol to be revoked from the mSig We have a long-term plan to move these permissions to the DAO smart contract with time-lock feature, controlled by the community in the decentralized way. This design is well-known to the public and is the same for all the Illuvium smart contracts, including Illuvium Token itself,

Staking contracts, and others; these contracts are operating in the mainnet for more then a year, admin transactions from our mSig are transparent

Multi-sign proxy address:
https://etherscan.io/address/0xBc83a1dCc9352F4C9Aa7e9CF5A47e01D369dF87a

LSI-02 | `_pauseDuration` Incorrectly Emitted

Category	Severity	Location	Status
Logical Issue	Informational	contracts/protocol/LandSale.sol: 629	Resolved

Description

In the function `initialize()`, when the sale is in paused state, the value of `_pauseDuration` will be incorrectly emitted in the `Resumed` event.

Recommendation

Consider emitting `pauseDuration + now32() - pausedAt` in the event.

Alleviation

`[CertiK]`: The team heeded the advice and merged the change into the master. Final commit hash to be provided by the team after all the issues are fixed and merged.

LSP-01 | Hardcoded Oracle Answer Update Timeframe

Category	Severity	Location	Status
Coding Style	Minor	contracts/protocol/LandSalePriceOracleV1.sol: 81	Resolved

Description

The oracle update timeframe is hardcoded as 30 days, which lacks of readability and maintenance

Recommendation

Consider creating a variable and setter for the oracle answer update timeframe.

Alleviation

`[CertiK]`: The team heeded the advice and merged the change into the master. Final commit hash to be provided by the team after all the issues are fixed and merged.

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.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

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.