DeHacker

Code Security Assessment

CeluvPlay

Sep 21th, 2023

Contents

Summary

2

DeHacker's objective was to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices.
Possible issues we looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Mishandled exceptions and call stack limits
- Unsafe external calls
- Integer overflow/underflow
- Number rounding errors
- Reentrancy and cross-function vulnerabilities
- Denial of service/logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting

Issue Categories

Every issue in this report was assigned a severity level from the following:

Critical severity issues

A vulnerability that can disrupt the contract functioning in a number of scenarios or creates a risk that the contract may be broken.

Major severity issues

A vulnerability that affects the desired outcome when using a contract or provides the opportunity to use a contract in an unintended way.

Medium severity issues

A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.

Minor severity issues

A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.

Informational

A vulnerability that has informational character but is not affecting any of the code.

Overview

Project Summary

Project Name	CeluvPlay
Platform	Polygon
Website	https://celuvplay.io/
Type	Infrastructure
Language	Solidity

Vulnerability Summary

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

Audit scope

ID	File	SHA256 Checksum
CEL	Celb.sol	df1e439b1b6b1a498d43b11c87cf01b43dba2770c0ede46acac1e978890c40a1
ERC	ERC20.sol	854ae83707f284d7b81bbdb93d687e2e67104e25583b8f1abcbaeba86a4462e9
ERB	ERC20Burnable.sol	1fc3dc5cac1aa6f395d897458f9a4534767a258cfc13d79bb9372a1e8474f1d7
ERL	ERC20Lockable.sol	c4b6a6bd68843d3869065baa780133fe4b23454348aa487122af8c2839965d19
OWN	Ownable.sol	10fec6fce1f90d57af3a4273efab322c186ef98c76bdaaf2670b28e7f2c104d8
PAU	Pausable.sol	15127ee28b484985527cc26051192d8e940d562b32f73aa5c6680b84421d3332

Findings

| ID	Category	Severity	Status
OX3-01	Centralization / Privilege	Major	Acknowledged
CEL-01	Logical Issue	Major	Acknowledged

MAJOR

OX3-O1 | Centralization Risks In ERC2OLockable.Sol

Category	Severity	Location	Status
Centralization / Privilege	Major	ERC2OLockable.sol : 66, 80; Ownable. sol; Pausable.sol	Acknowledged

Description

In the contract Ownable the role _owner has authority over the functions shown in the diagram below. Anycompromise to the _owner account may allow the hacker to take advantage of this authority.
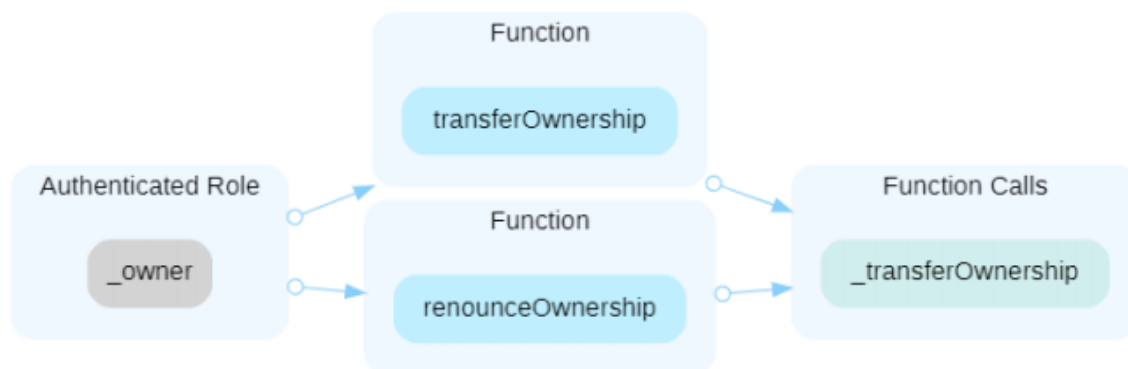
In the contract Pausable the role _owner has authority over the functions shown in the diagram below. Anycompromise to the _owner account may allow the hacker to take advantage of this authority.
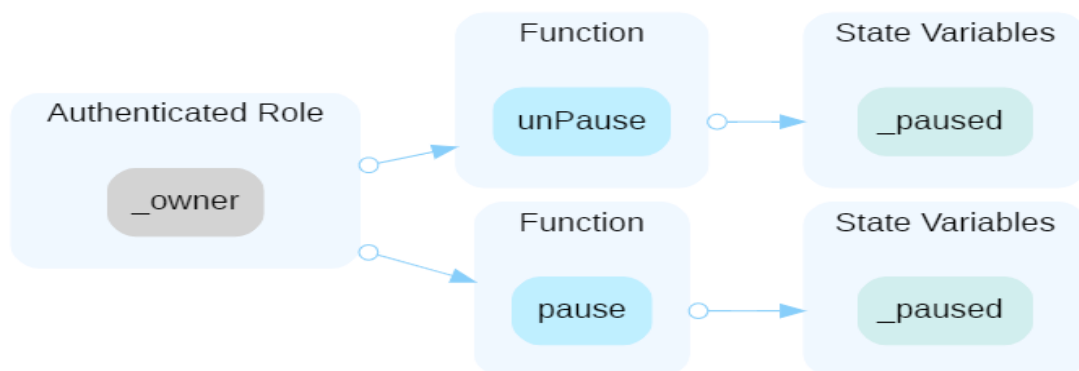
In the contract ERC2OLockable the role _owner has authority over the functions shown in the diagrambelow. Any compromise to the _owner account may allow the hacker to take advantage of this authority.

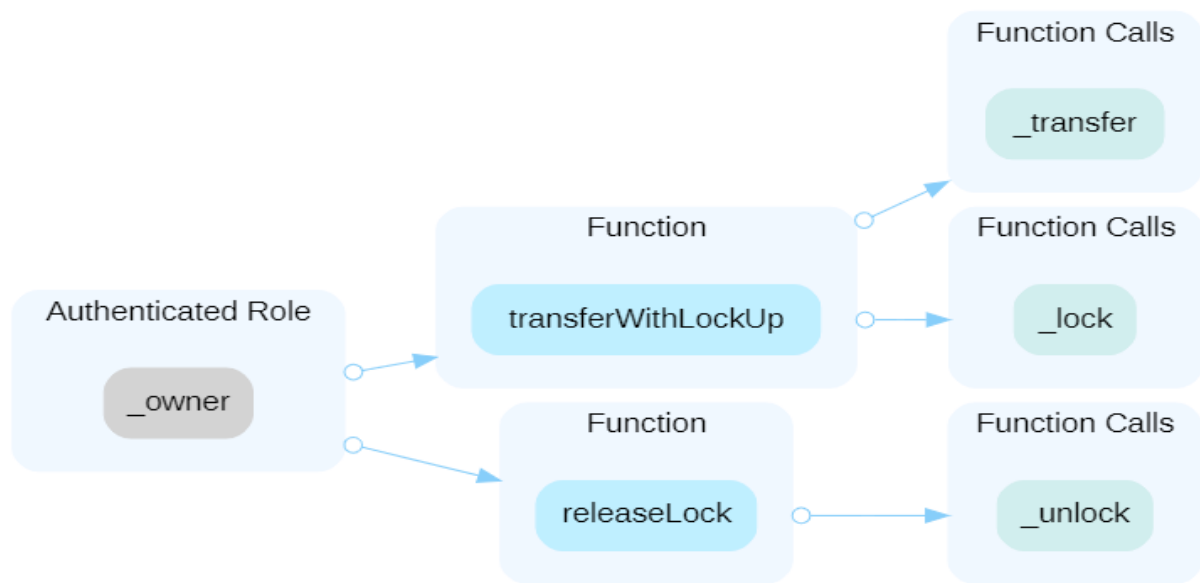## Recommendation

The risk describes the current project design and potentially makes iterations to improve in the securityoperation and level of decentralization, which in most cases cannot be resolved entirely at the presentstage. We advise the client to carefully manage the privileged account's private key to avoid any potentialrisks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol beimproved via a decentralized mechanism or smart-contract-based accounts with enhanced securitypractices, e.g., multisignature wallets. Indicatively, here are some feasible suggestions that would alsomitigate the potential risk at a different level in terms of short-term, long-term and permanent:

Short Term:

Timelock and Multi sign (,) combination mitigate by delaying the sensitive operation and avoiding asingle 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 theprivate key compromised;

AND

A medium/blog link for sharing the timelock contract and multi-signers addresses information with thepublic audience.CeluvPlay Security Assessment

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 informationwith 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

MAJOR

CEL-O1 | Initial Token Distribution

Category	Severity	Location	Status
Logical Issue	Major	Celb.sol	Acknowledged

Description

All of the CELB tokens are sent to the contract deployer when deploying the contract. This could be acentralization risk as the deployer can distribute CELB tokens without obtaining the consensus of thecommunity.

Recommendation

We recommend the team to be transparent regarding the initial token distribution process, and the teamshall make enough efforts to restrict the access of the private key.

Disclaimer

This report is based on the scope of materials and documentation provided for a limited review at the time provided. Results may not be complete nor inclusive of all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Blockchain technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. A report does not indicate the endorsement of any particular project or team, nor guarantee its security. No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, we disclaim all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate.

FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

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.

Coding Style

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

Volatile Code

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

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.

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.

About

DeHacker is a team of auditors and white hat hackers who perform security audits and assessments. With decades of experience in security and distributed systems, our experts focus on the ins and outs of system security. Our services follow clear and prudent industry standards. Whether it's reviewing the smallest modifications or a new platform, we'll provide an in-depth security survey at every stage of your company's project. We provide comprehensive vulnerability reports and identify structural inefficiencies in smart contract code, combining high-end security research with a real-world attacker mindset to reduce risk and harden code.

BLOCKCHAIINS

Ethereum   Cosmos

Eos   Substrate

TECH STACK

Python   Solidity

Rust   C++

CONTACTS

https://dehacker.io

https://twitter.com/dehackerio

https://github.com/dehacker/audits_public

https://t.me/dehackerio

https://blog.dehacker.io/

Sep 2023