⚠ **Disclaimer** Not a financial advice.Always DYOR.

Latest Audit - 2023/01/31

Z3

0x50Eec6D765792dCfB0913C8403ef2A12e1B861a6

Static analysis Dynamic analysis Symbolic Execution SWC check

Z³ is a decentralised, zero-emission, Proof of Holdings (POH), auto-mining protocol on the ethereum blockchain. Buy, Hold, Mine, Grow.

CONTRACT ADDRESS 0x50Ee...B861a6	NETWORK Ethereum Mainnet	LICENSE MIT	COMPILER v0.8.17+commit.8df45f5f
TYPE N/A	LANGUAGE Solidity	REQUEST DATE 2023/01/29	REVISION DATE 2023/01/31

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL	OPTIMIZATION
✓ Passed	✓ Passed	✓ Passed	✗ 3 Issues	✓ Passed	✓ Passed

Owner privileges

No critical issues found
The contract does not contain issues of high or medium criticality. This means that no known vulnerabilities were found in the source code. ✓

Contract owner cannot mint
It is not possible to mint new tokens. ✓

Contract owner cannot blacklist addresses.
It is not possible to lock user funds by blacklisting addresses. ✓

Contract owner cannot set high fees
The fees, if applicable, can be a maximum of 25% or lower. The contract can therefore not be locked. Please take a look in the comment section for more details. ✓

Contract cannot be locked
Owner cannot lock any user funds. ✓

Token cannot be burned
There is no burn function within the contract. ✓

Ownership is not renounced
Contract can be manipulated by owner functions. ✗

Comments

Ownership Privileges:

- Change/Update the pair token and the AMM address
- Disable limits and transfer delay but cannot re-enable them
- Enable Trading but cannot disable it
- Add/Remove wallets from fee exemption
- Set fees and Fee receiver addresses.
- Withdraw tokens from the contract but not native ones.
- Set the next rebase in the future with any date.

Due to lack of access control, any user can call the manual rebase function whenever the next rebase time is reached or passed.

We recommend investors/users to do their own research before investing

Audit Scope

This audit covered the following files listed below with a SHA-1 Hash. The above token Team provided us with the files that needs to be tested.

We will verify the following claims:

- Correct implementation of Token standard
- Deployer cannot mint any new tokens
- Deployer cannot burn or lock user funds
- Deployer cannot pause the contract
- Overall checkup (Smart Contract Security)

The auditing process follows a routine series of steps:

- Review of the specifications, sources, and instructions provided to SolidProof to make sure we understand the size, scope, and functionality of the smart contract.
- Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to SolidProof describe.
- Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
- Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
- Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
- Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts.

A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

ZCubed.sol

`b69b2896930efdc364b0145237a73a94b11ce8bd`

Audit Details

Throughout the review process, care was taken to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as there were discovered.

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Low Issues

#1 ISSUE ⓘ

⌛ Pending

Missing Events Arithmetic (events-maths)

ZCUBED.SOL

L736-742 L749-752

DESCRIPTION

Emit an event for critical parameter changes.

#2 ISSUE ⓘ

⌛ Pending

Uninitialized local variables (uninitialized-local)

ZCUBED.SOL

L383 L384

DESCRIPTION

Initialize all the variables. If a variable is meant to be initialized to zero, explicitly set it to zero to improve code readability.

#3 ISSUE ⓘ

⌛ Pending

Dangerous usage of `tx.origin` (tx-origin)

ZCUBED.SOL

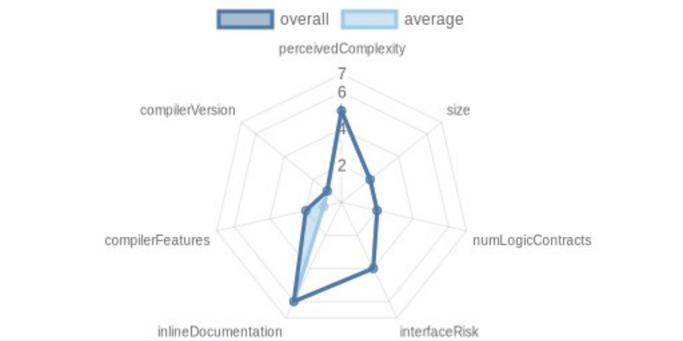
L497-544

DESCRIPTION

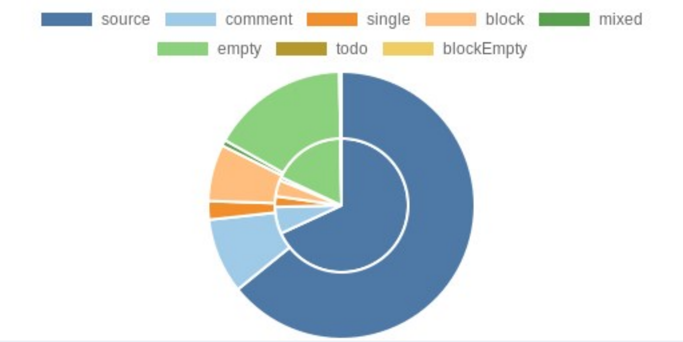
Do not use `tx.origin` for authorization.

Diagrams

Risk Chart



Source Lines Chart



Disclaimer

SolidProof.io reports are not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc’...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug- free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing 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. SolidProof’s position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of security or functionality of the technology we agree to analyze.