



d3ploy



SECURITY ASSESSMENT

Zebec Protocol

November 13th 2022

TABLE OF
Contents

01 Legal Disclaimer

02 D3ploy Intro

03 Project Summary

04 Audit Score

05 Audit Scope

06 Methodology

07 Key Findings

08 Vulnerabilities

09 Source Code

10 Appendix

LEGAL

Disclaimer

D3ploy audits 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 or project that contracts d3ploy to perform a security review. D3ploy 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.

D3ploy 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. The report is provided only for the contract(s) mentioned in the report and does not include any other potential additions and/or contracts deployed by Owner. The report does not provide a review for contract(s), applications and/or operations, that are out of this report scope.

D3ploy’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.

D3ploy represents 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. D3ploy’s position is that each company and individual are responsible for their own due diligence and continuous security. The security audit is not meant to replace functional testing done before a software release. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent manual audits and a public bug bounty program to ensure the security of the smart contracts.

D3PLOY

Introduction

D3ploy 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.

Secure your project with d3ploy

We offer field-proven audits with in-depth reporting and a range of suggestions to improve and avoid contract vulnerabilities. Industry-leading comprehensive and transparent smart contract auditing on all public and private blockchains.



Vulnerability checking

A crucial manual inspection carried out to eliminate any code flaws and security loopholes. This is vital to avoid vulnerabilities and exposures incurring costly errors at a later stage.



Contract verification

A thorough and comprehensive review in order to verify the safety of a smart contract and ensure it is ready for launch and built to protect the end-user



Risk assessment

Analyse the architecture of the blockchain system to evaluate, assess and eliminate probable security breaches. This includes a full assessment of risk and a list of expert suggestions.



In-depth reporting

A truly custom exhaustive report that is transparent and depicts details of any identified threats and vulnerabilities and classifies those by severity.



Fast turnaround

We know that your time is valuable and therefore provide you with the fastest turnaround times in the industry to ensure that both your project and community are at ease.



Best-of-class blockchain engineers

Our engineers combine both experience and knowledge stemming from a large pool of developers at our disposal. We work with some of the brightest minds that have audited countless smart contracts over the last 4 years.

PROJECT

Introduction

Zebec is a multi-chain continuous Settlement Protocol that will transform payroll, cash flow, and token vesting by allowing users to send payments and distributions every second. Launching the world's first on-chain payroll product with full tax withholding built-in and the first debit card for Solana wallets.

Zebec is enabling composable transfer of value starting with Zebec Payroll. Zebec Safe is fully customizable multi-sig on Solana. A revolutionary DeFi technology that empowers real-time, frictionless and continuous streams of payments.

Project Name **Zebec Protocol**

Contract Name **ZBC Token**

Contract Address **zebeczgi5fSEtbpfQKVZKCJ3WgYXxjkMUKNNx7fLKAF**

Contract Chain **Mainnet**

Contract Type **Smart Contract**

Platform **Solana**

Language **Rust**

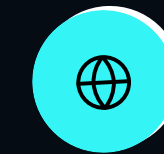
Network **Solana (SOL) & BNB Chain (BEP20)**

Codebase **Private GitHub Repository**

Total Token Supply **10,000.000.000**

INFO

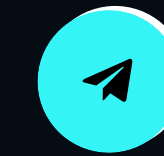
Social



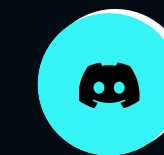
<https://zebec.io/>



https://twitter.com/Zebec_HQ



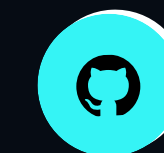
<https://t.me/zebececosystem>



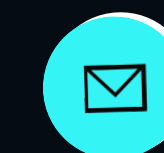
<https://discord.com/jUwZ3cHauZ>



-



<https://github.com/Zebec-protocol>



-



AUDIT

Score

◆ Issues	1
◆ Critical	0
◆ Major	0
◆ Medium	0
◆ Minor	0
◆ Informational	1
◆ Discussion	0

All issues are described in further detail on the following pages.

AUDIT Scope

CODEBASE FILES

Zebec-protocol/wzbc-contract/programs/wzbc_anchor/src/lib.rs

LOCATION

✦ Private Repository

REVIEW Methodology

TECHNIQUES

This report has been prepared for Zebec Protocol to discover issues and vulnerabilities in the source code of the Zebec Protocol project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Dynamic, 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 major 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 in the comments below.

TIMESTAMP

Version *v1.0*

Date *2022/11/13*

Description *Layout project*

Architecture / Manual review / Static & dynamic security testing

Final Summary

KEY Finding

TITLE

Dead Code

SEVERITY

✦ Informational

STATUS

Acknowledged

DESCRIPTION

It is recommended to keep the production repository clean to prevent confusion and the introduction of vulnerabilities. The functions and parameters, contracts, and interfaces that are never used or called externally or from inside the contracts should be removed when the contract is deployed on the mainnet.

AFFECTED CODE

- `std::str::FromStr` [L18](#)
- `zbc_mint`
- `payer_wzebec_account`
- `ZBC_ADDRESS`
- `WZBC_ADDRESS`

IMPACTS

This does not impact the security aspect of the Smart contract but prevents confusion when the code is sent to other developers or auditors to understand and implement. This reduces the overall size of the contracts and also helps in saving gas.

Issue : Dead Code

Type : Code With No Effects – SWC-135

<https://swcregistry.io/docs/SWC-135>

Level : Informational

Remediation : If the variables and constants are not supposed to be used anywhere, consider removing them from the contract.

Alleviation / Retest : Zebec Protocol team has acknowledged the issue.

SOURCE Code

Private GitHub Repository

WEBSITE d3ploy.co



[@d3ploy_](https://twitter.com/d3ploy_) TWITTER

REPORT Appendix

FINDING CATEGORIES

The assessment process will utilize a mixture of static analysis, dynamic analysis, in-depth manual review and/or other security techniques.

This report has been prepared for Zebec Protocol project using the above techniques to examine and discover vulnerabilities and safe coding practices in Zebec Protocol's smart contract including the libraries used by the contract that are not officially recognized.

A comprehensive static and dynamic analysis has been performed on the solidity code in order to find vulnerabilities ranging from minor gas optimizations to major vulnerabilities leading to the loss of funds.

Various common and uncommon attack vectors will be investigated to ensure that the smart contracts are secure from malicious actors. The testing methods find and flag issues related to gas optimizations that help in reducing the overall gas cost It scans and evaluates the codebase against industry best practices and standards to ensure compliance It makes sure that the officially recognized libraries used in the code are secure and up to date.

AUDIT SCORES

D3ploy Audit Score is not a live dynamic score. It is a fixed value determined at the time of the report issuance date.

D3ploy Audit Score is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. These reports and scores are 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 d3ploy to perform a security review.



d3ploy

WEBSITE d3ploy.co

[@d3ploy_](https://twitter.com/d3ploy_) TWITTER