Paxos YBS

Security Assessment (Summary Report)

February 20, 2024

Prepared for:
Henryk Sarat
Paxos

Prepared by: **Justin Jacob and Damilola Edwards**

About Trail of Bits

Founded in 2012 and headquartered in New York, Trail of Bits provides technical security assessment and advisory services to some of the world's most targeted organizations. We combine high-end security research with a real-world attacker mentality to reduce risk and fortify code. With 100+ employees around the globe, we've helped secure critical software elements that support billions of end users, including Kubernetes and the Linux kernel.

We maintain an exhaustive list of publications at https://github.com/trailofbits/publications, with links to papers, presentations, public audit reports, and podcast appearances.

In recent years, Trail of Bits consultants have showcased cutting-edge research through presentations at CanSecWest, HCSS, Devcon, Empire Hacking, GrrCon, LangSec, NorthSec, the O'Reilly Security Conference, PyCon, REcon, Security BSides, and SummerCon.

We specialize in software testing and code review projects, supporting client organizations in the technology, defense, and finance industries, as well as government entities. Notable clients include HashiCorp, Google, Microsoft, Western Digital, and Zoom.

Trail of Bits also operates a center of excellence with regard to blockchain security. Notable projects include audits of Algorand, Bitcoin SV, Chainlink, Compound, Ethereum 2.0, MakerDAO, Matic, Uniswap, Web3, and Zcash.

To keep up to date with our latest news and announcements, please follow @trailofbits on Twitter and explore our public repositories at https://github.com/trailofbits. To engage us directly, visit our "Contact" page at https://www.trailofbits.com/contact, or email us at info@trailofbits.com.

Trail of Bits, Inc.
497 Carroll St., Space 71, Seventh Floor
Brooklyn, NY 11215
https://www.trailofbits.com
info@trailofbits.com

Notices and Remarks

Copyright and Distribution

Test Coverage Disclaimer

All activities undertaken by Trail of Bits in association with this project were performed in accordance with a statement of work and agreed upon project plan.

Security assessment projects are time-boxed and often reliant on information that may be provided by a client, its affiliates, or its partners. As a result, the findings documented in this report should not be considered a comprehensive list of security issues, flaws, or defects in the target system or codebase.

Trail of Bits uses automated testing techniques to rapidly test the controls and security properties of software. These techniques augment our manual security review work, but each has its limitations: for example, a tool may not generate a random edge case that violates a property or may not fully complete its analysis during the allotted time. Their use is also limited by the time and resource constraints of a project.

Table of Contents

Project Summary

Contact Information

The following project manager was associated with this project:

Anne Marie Barry, Project Manager
annemarie.barry@trailofbits.com

The following engineering director was associated with this project:

Josselin Feist, Engineering Director, Blockchain
josselin.feist@trailofbits.com

The following consultants were associated with this project:

Justin Jacob, Consultant
justin.jacob@trailofbits.com

Damilola Edwards, Consultant
damilola.edwards@trailofbits.com

Project Timeline

The significant events and milestones of the project are listed below.

Date	Event
February 13, 2024	Pre-project kickoff call
February 20, 2024	Delivery of report draft
February 20, 2024	Report readout meeting
February XX, 2024	Delivery of summary report

Project Targets

The engagement involved a review and testing of the target listed below.

ybs-contract-audit

Repository	https://github.com/paxosglobal/ybs-contract-audit
Versions	`5a369c318b5985ea9d69af50e7c51212fc46fa28`
	`2c94915254f73bf0afd26054a545297e38d956ec`
Type	Solidity
Platform	EVM

Executive Summary

Engagement Overview

Paxos engaged Trail of Bits to review the security of its Yield-Bearing Stablecoin (YBS). The YBS is designed to give YBS holders yield by periodically rebasing and increasing in value according to a multiplier set by the Paxos team.

A team of two consultants conducted the review from February 12 to February 16, 2024, for a total of two engineer-weeks of effort. With full access to source code and documentation, we performed static and dynamic testing of the codebase, using automated and manual processes.

Observations and Impact

Overall, the codebase is relatively simple and easy to understand. We reviewed the codebase's access controls, ERC-20 conformance, and rebasing mechanism, focusing on the correctness of the implementation. While we did not identify any high-severity issues, we did find informational-severity issues related to front-running, lack of event emissions, and lack of upper bound enforcement. The codebase contains good NatSpec documentation, and the project's README provides a good description about the roles used and their various permissions.

Recommendations

Based on the findings and codebase maturity evaluation in this report, we recommend that Paxos take the following steps:

- **Remediate the findings disclosed in this report.** These findings should be addressed as part of a direct remediation or as part of any refactor that may occur when addressing other recommendations.
- **Add a stateful fuzzing test suite.** Trail of Bits considers stateful fuzzing to be a baseline requirement for DeFi protocols and applications and recommends fuzzing the system's user flows and arithmetic calculations.

  Guidance on introducing stateful fuzzing can be found in Trail of Bits' "Learn how to fuzz like a pro" series on YouTube.

Codebase Maturity Evaluation

Trail of Bits uses a traffic-light protocol to provide each client with a clear understanding of the areas in which its codebase is mature, immature, or underdeveloped. Deficiencies identified here often stem from root causes within the software development life cycle that should be addressed through standardization measures (e.g., the use of common libraries, functions, or frameworks) or training and awareness programs.

Category	Summary	Result
Arithmetic	The system uses simple and easy-to-understand arithmetic. However, we recommend implementing arithmetic and roundtrip fuzzing of the math functions to ensure consistency and robustness of operations throughout the codebase.	**Satisfactory**
Auditing	Most state-changing operations correctly emit events. The Paxos team provided a detailed incident response plan as part of its internal process documentation. However, we found one operation that does not emit an event (TOB-YBS-2), it is also unclear how the Paxos team handles these events.	**Moderate**
Authentication / Access Controls	The roles in the contract use the role-based access controls pattern, which is easy to understand and has clear separation of powers. The roles have immense power over the system. Further documentation on the actions roles will take and the frequency these actions will occur would make the system's inner workings more transparent to users.	**Satisfactory**
Complexity Management	The contract is a simple ERC-20 token implementing EIP-2612 and EIP-3309 as well as a rebasing feature. The components are simple and adhere to the specification. Furthermore, the logic is cleanly separated, allowing each function to be easy to understand.	**Satisfactory**
Decentralization	The roles throughout the system have immense power, including the ability to block users from receiving yield and to arbitrarily seize user assets. It is presumed that the Paxos team will control these roles; however, it is unclear whether the accounts that contain these roles	**Weak**

	will be controlled by a centralized actor or a multisignature wallet. Further transparency is essential to garner user trust in the system.	
Documentation	The codebase contains sufficient NatSpec documentation and documentation about how rebasing is performed. The Paxos team provided elaborate documentation on the system technical details and deployment process. The project's README provides adequate documentation on the privileges and permissions. However, further guidance about exactly how important variables in the contracts will be updated by the Paxos team could be provided to give users stronger guarantees about the system.	**Satisfactory**
Low-Level Manipulation	The contracts do not use any low-level manipulation.	**Strong**
Testing and Verification	While the codebase does have sufficient unit tests and some simple fuzz tests, the protocol lacks stateful and arithmetic fuzz testing. Implementing further fuzz testing will be crucial for identifying potential edge cases and unexpected behavior in the contracts.	**Moderate**
Transaction Ordering	We found one issue regarding transaction reordering risks (TOB-YBS-1). We recommend that the Paxos team investigate the codebase for transaction reordering opportunities and either document them if they are unavoidable or refactor the code to limit their impact.	**Moderate**

Summary of Findings

The table below summarizes the findings of the review, including type and severity details.

ID	Title	Type	Severity
1	Transaction reordering opportunity that can enable arbitrage before/after a rebase	Timing	**Low**
2	Lack of event emission in _updateAfterIncrMultIfRequired	Auditing and Logging	**Informational**
3	Lack of upper bound check in setRebasePeriod	Data Validation	**Informational**

A. Code Maturity Categories

The following tables describe the code maturity categories and rating criteria used in this document.

Code Maturity Categories	
Category	**Description**
Arithmetic	The proper use of mathematical operations and semantics
Auditing	The use of event auditing and logging to support monitoring
Authentication / Access Controls	The use of robust access controls to handle identification and authorization and to ensure safe interactions with the system
Complexity Management	The presence of clear structures designed to manage system complexity, including the separation of system logic into clearly defined functions
Cryptography and Key Management	The safe use of cryptographic primitives and functions, along with the presence of robust mechanisms for key generation and distribution
Decentralization	The presence of a decentralized governance structure for mitigating insider threats and managing risks posed by contract upgrades
Documentation	The presence of comprehensive and readable codebase documentation
Low-Level Manipulation	The justified use of inline assembly and low-level calls
Testing and Verification	The presence of robust testing procedures (e.g., unit tests, integration tests, and verification methods) and sufficient test coverage
Transaction Ordering	The system's resistance to transaction-ordering attacks

Rating Criteria	
Rating	**Description**
Strong	No issues were found, and the system exceeds industry standards.
Satisfactory	Minor issues were found, but the system is compliant with best practices.
Moderate	Some issues that may affect system safety were found.

Weak	Many issues that affect system safety were found.
Missing	A required component is missing, significantly affecting system safety.
Not Applicable	The category is not applicable to this review.
Not Considered	The category was not considered in this review.
Further Investigation Required	Further investigation is required to reach a meaningful conclusion.

E. Fix Review Results

When undertaking a fix review, Trail of Bits reviews the fixes implemented for issues identified in the original report. This work involves a review of specific areas of the source code and system configuration, not comprehensive analysis of the system.

On March 1, 2024, Trail of Bits reviewed the fixes and mitigations implemented by the Paxos team for the issues identified in this report. We reviewed each fix to determine its effectiveness in resolving the associated issue.

In summary, of the three issues described in this report, the Paxos team has resolved one issue and has not resolved the remaining two issues. For additional information, please see the Detailed Fix Review Results below.

ID	Title	Status
1	Transaction reordering opportunity that can enable arbitrage before/after a rebase	Unresolved
2	Lack of event emission in _updateAfterIncrMultIfRequired	Resolved
3	Lack of upper bound check in setRebasePeriod	Unresolved

Detailed Fix Review Results

TOB-YBS-1: Transaction reordering opportunity that can enable arbitrage before/after a rebase
Unresolved. The client provided the following context for this finding's fix status:

> *Paxos will update the documentation, making token holders aware of arbitrage opportunities.*

TOB-YBS-2: Lack of event emission in _updateAfterIncrMultIfRequired
Resolved in commit 3b1d84c. The `_updateAfterIncrMultRequired` function was updated to emit an event.

TOB-YBS-3: Lack of upper bound check in setRebasePeriod
Unresolved. The client provided the following context for this finding's fix status:

> *Paxos does not desire the rebase period to be bounded. The role controlling the `setRebasePeriod` method will be set to a multisignature wallet. Signers will have to agree upon the period; therefore, no single signer will be able arbitrarily set the rebase period.*

F. Fix Review Status Categories

The following table describes the statuses used to indicate whether an issue has been sufficiently addressed.

Fix Status	
Status	**Description**
Undetermined	The status of the issue was not determined during this engagement.
Unresolved	The issue persists and has not been resolved.
Partially Resolved	The issue persists but has been partially resolved.
Resolved	The issue has been sufficiently resolved.