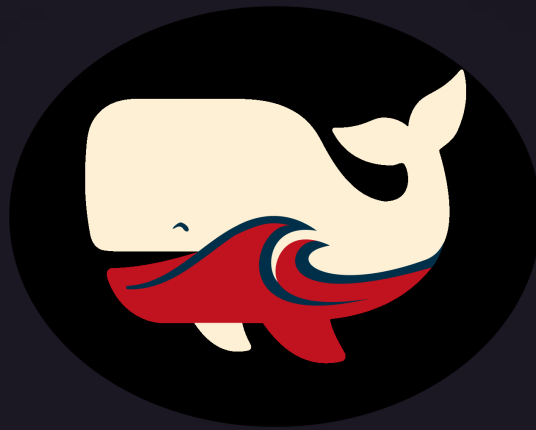




Security Review For Boardwalk



Collaborative Audit Prepared For:
Lead Security Expert(s):

Boardwalk
LZ_security
vinica_boy

Date Audited:

July 4 - July 7, 2026

Introduction

Security Review focusing on the CCA for secure deployment.

Scope

Repository: useboardwalk/boardwalk-contracts

Audited Commit: 29b1610fc71f281248d274a7fa05d302b4c114d9

Final Commit: 94faac7702597eef50c75df4ed95438bc56afb95

Files:

- src/governance/GovernanceVoter.sol
- src/governance/LPLocker.sol
- src/token/BwsMigration.sol
- src/token/BWS.sol
- src/token/UnsoldBurner.sol

Final Commit Hash

94faac7702597eef50c75df4ed95438bc56afb95

Findings

Each issue has an assigned severity:

- High issues are directly exploitable security vulnerabilities that need to be fixed.
- Medium issues are security vulnerabilities that may not be directly exploitable or may require certain conditions in order to be exploited. All major issues should be addressed.
- Low/Info issues are non-exploitable, informational findings that do not pose a security risk or impact the system's integrity. These issues are typically cosmetic or related to compliance requirements, and are not considered a priority for remediation.

Issues Found

High	Medium	Low/Info
0	0	0

Issues Not Fixed and Not Acknowledged

High	Medium	Low/Info
0	0	0

No issues identified

Over the course of this Security Review, beyond the thorough analysis of the the contract code itself for `GovernanceVoter.sol` and `BwsMigration.sol`, particular emphasis was placed on whether the migration process could introduce new issues and attack vectors.

As for `LPLocker.sol`, `BWS.sol`, and `UnsoldBurner.sol`, the review focused primarily on the contracts themselves and their integration and interaction with the CCA.

No issues have been identified in the code or the migration process. The contracts are well-structured, and the logic is sound. The migration process has been designed to ensure that all necessary state is preserved and that no new vulnerabilities are introduced.

This report is signed off on by the Security Researcher team and Sherlock.

Disclaimers

Sherlock does not provide guarantees nor warranties relating to the security of the project.

Usage of all smart contract software is at the respective users' sole risk and is the users' responsibility.