Aderyn Analysis Report

This report was generated by Aderyn, a static analysis tool built by Cyfrin, a blockchain security company. This report is not a substitute for manual audit or security review. It should not be relied upon for any purpose other than to assist in the identification of potential security vulnerabilities.

Table of Contents

- Summary
  - Files Summary
  - Files Details
  - Issue Summary
- High Issues
  - H-1: Arbitrary `from` passed to `transferFrom` (or `safeTransferFrom`)
- Low Issues
  - L-1: Centralization Risk for trusted owners
  - L-2: Unsafe ERC20 Operations should not be used
  - L-3: Missing checks for `address(0)` when assigning values to address state variables
  - L-4: `public` functions not used internally could be marked `external`
  - L-5: Event is missing `indexed` fields
  - L-6: PUSH0 is not supported by all chains

Summary

Files Summary

Key	Value
.sol Files	4
Total nSLOC	101

Files Details

Filepath	nSLOC
src/L1BossBridge.sol	64
src/L1Token.sol	8
src/L1Vault.sol	12
src/TokenFactory.sol	17
Total	**101**

Issue Summary

Category	No. of Issues
High	1
Low	6

High Issues

H-1: Arbitrary `from` passed to `transferFrom` (or `safeTransferFrom`)

Passing an arbitrary `from` address to `transferFrom` (or `safeTransferFrom`) can lead to loss of funds, because anyone can transfer tokens from the `from` address if an approval is made.

- Found in src/L1BossBridge.sol Line: 74

```
        token.safeTransferFrom(from, address(vault), amount);
```

Low Issues

L-1: Centralization Risk for trusted owners

Contracts have owners with privileged rights to perform admin tasks and need to be trusted to not perform malicious updates or drain funds.

- Found in src/L1BossBridge.sol Line: 27

```
contract L1BossBridge is Ownable, Pausable, ReentrancyGuard {
```

- Found in src/L1BossBridge.sol Line: 49

```
    function pause() external onlyOwner {
```

- Found in src/L1BossBridge.sol Line: 53

```
    function unpause() external onlyOwner {
```

- Found in src/L1BossBridge.sol Line: 57

```
    function setSigner(address account, bool enabled) external onlyOwner {
```

- Found in src/L1Vault.sol Line: 12

```
contract L1Vault is Ownable {
```

- Found in src/L1Vault.sol Line: 19

```
    function approveTo(address target, uint256 amount) external onlyOwner {
```

- Found in src/TokenFactory.sol Line: 11

```
contract TokenFactory is Ownable {
```

- Found in src/TokenFactory.sol Line: 23

```
    function deployToken(string memory symbol, bytes memory
contractBytecode) public onlyOwner returns (address addr) {
```

L-2: Unsafe ERC20 Operations should not be used

ERC20 functions may not behave as expected. For example: return values are not always meaningful. It is recommended to use OpenZeppelin's SafeERC20 library.

- Found in src/L1BossBridge.sol Line: 99

```
                abi.encodeCall(IERC20.transferFrom, (address(vault), to,
amount))
```

- Found in src/L1Vault.sol Line: 20

```
        token.approve(target, amount);
```

L-3: Missing checks for `address(0)` when assigning values to address state variables

Check for `address(0)` when assigning values to address state variables.

- Found in src/L1BossBridge.sol Line: 58

```
        signers[account] = enabled;
```

- Found in src/L1Vault.sol Line: 16

```
        token = _token;
```

L-4: `public` functions not used internally could be marked `external`

Instead of marking a function as `public`, consider marking it as `external` if it is not used internally.

- Found in src/TokenFactory.sol Line: 23

```
    function deployToken(string memory symbol, bytes memory
contractBytecode) public onlyOwner returns (address addr) {
```

- Found in src/TokenFactory.sol Line: 31

```
    function getTokenAddressFromSymbol(string memory symbol) public view
returns (address addr) {
```

L-5: Event is missing `indexed` fields

Index event fields make the field more quickly accessible to off-chain tools that parse events. However, note that each index field costs extra gas during emission, so it's not necessarily best to index the maximum allowed per event (three fields). Each event should use three indexed fields if there are three or more fields, and gas usage is not particularly of concern for the events in question. If there are fewer than three fields, all of the fields should be indexed.

- Found in src/L1BossBridge.sol Line: 40

```
    event Deposit(address from, address to, uint256 amount);
```

- Found in src/TokenFactory.sol Line: 14

```
    event TokenDeployed(string symbol, address addr);
```

L-6: PUSH0 is not supported by all chains

Solc compiler version 0.8.20 switches the default target EVM version to Shanghai, which means that the generated bytecode will include PUSH0 opcodes. Be sure to select the appropriate EVM version in case you

intend to deploy on a chain other than mainnet like L2 chains that may not support PUSH0, otherwise deployment of your contracts will fail.

- Found in src/L1BossBridge.sol Line: 15

```
pragma solidity 0.8.20;
```

- Found in src/L1Token.sol Line: 2

```
pragma solidity 0.8.20;
```

- Found in src/L1Vault.sol Line: 2

```
pragma solidity 0.8.20;
```

- Found in src/TokenFactory.sol Line: 2

```
pragma solidity 0.8.20;
```