BOB USDC Bridge Security Review

Pashov Audit Group

Conducted by: 0xunforgiven, carrotsmuggler, SpicyMeatball

April 19th 2024 - April 22th 2024

Contents

1. About Pashov Audit Group

Pashov Audit Group consists of multiple teams of some of the best smart contract security researchers in the space. Having a combined reported security vulnerabilities count of over 1000, the group strives to create the absolute very best audit journey possible - although 100% security can never be guaranteed, we do guarantee the best efforts of our experienced researchers for your blockchain protocol. Check our previous work here or reach out on Twitter @pashovkrum.

2. Disclaimer

A smart contract security review can never verify the complete absence of vulnerabilities. This is a time, resource and expertise bound effort where we try to find as many vulnerabilities as possible. We can not guarantee 100% security after the review or even if the review will find any problems with your smart contracts. Subsequent security reviews, bug bounty programs and on-chain monitoring are strongly recommended.

3. Introduction

A time-boxed security review of the **bob-collective/optimism** repository was done by **Pashov Audit Group**, with a focus on the security aspects of the application's smart contracts implementation.

4. About BOB USDC Bridge

BOB is a hybrid Layer-2 powered by Bitcoin and Ethereum. The design is such that Bitcoin users can easily onboard to the BOB L2 without previously holding any Ethereum assets. The user coordinates with the trusted relayer to reserve some of the available liquidity, sends BTC on the Bitcoin mainnet and then the relayer can provide a merkle proof to execute a swap on BOB for an ERC20 token. The liquidity provider (LP) first locks that token in Onramp.sol as well as some small amount of ETH to allow that user to do some swaps on BOB. The LP receives Bitcoin to their specified address and can re-balance by converting that to the wrapped token and re-depositing.

5. Risk Classification

Severity	**Impact: High**	**Impact: Medium**	**Impact: Low**
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

5.1. Impact

- High - leads to a significant material loss of assets in the protocol or significantly harms a group of users.
- Medium - only a small amount of funds can be lost (such as leakage of value) or a core functionality of the protocol is affected.
- Low - can lead to any kind of unexpected behavior with some of the protocol's functionalities that's not so critical.

5.2. Likelihood

- High - attack path is possible with reasonable assumptions that mimic on-chain conditions, and the cost of the attack is relatively low compared to the amount of funds that can be stolen or lost.
- Medium - only a conditionally incentivized attack vector, but still relatively likely.
- Low - has too many or too unlikely assumptions or requires a significant stake by the attacker with little or no incentive.

5.3. Action required for severity levels

- Critical - Must fix as soon as possible (if already deployed)
- High - Must fix (before deployment if not already deployed)
- Medium - Should fix
- Low - Could fix

6. Security Assessment Summary

review commit hashes - 4c27e88204aaa8dc531b3ff1fdd5b4e8ec85d056

fixes review commit hashes - c9648bed367881438e782bf9e7de9dc70fa50a29

Scope

The following smart contracts were in scope of the audit:

- `IPartialUsdc`
- `L1UsdcBridge`
- `L2UsdcBridge`
- `UsdcBridge`
- `Pausable`
- `UsdcManager`

7. Executive Summary

Over the course of the security review, 0xunforgiven, carrotsmuggler, SpicyMeatball engaged with BOB to review BOB USDC Bridge. In this period of time a total of **1** issues were uncovered.

Protocol Summary

Protocol Name	BOB USDC Bridge
Repository	https://github.com/bob-collective/optimism
Date	April 19th 2024 - April 22th 2024
Protocol Type	Hybrid Layer 2

Findings Count

Severity	**Amount**
Low	1
Total Findings	**1**

Summary of Findings

ID	**Title**	**Severity**	**Status**
[L-01]	Bridged USDC Standard not fully complied	Low	Resolved

8. Findings

8.1. Low Findings

[L-01] Bridged USDC Standard not fully complied

docs link

The Bridged USDC standard specifies that the bridge should possess the capability to burn locked tokens.

> Burn the amount of USDC held by the bridge that corresponds precisely to the circulating total supply of bridged USDC established by the supply lock.

However, the current implementation burns all tokens held by the L1 bridge, even those that were not bridged (e.g. sent by mistake). This discrepancy may lead to differences in the supplies on L1 and L2.

```
function burnLockedUSDC() external {
        require(msg.sender == burner, "Not whitelisted");

        IPartialUsdc token = IPartialUsdc(l1Usdc);
>>      uint256 balance = token.balanceOf(address(this));
        token.burn(balance);
    }
```

Consider burning only locked tokens:

```
+       uint256 balance = deposits[l1Usdc][l2Usdc];
        token.burn(balance);
```