Orange
Audit Report

Mon Jul 08 2024

✉ contact@bitslab.xyz https://twitter.com/scalebit_

ScaleBit

Orange Audit Report

1 Executive Summary

1.1 Project Information

Description	Orange is the first BTC Layer 2 solution featuring PoW mining
Type	L2
Auditors	ScaleBit
Timeline	Thu Jul 04 2024 - Mon Jul 08 2024
Languages	Solidity
Platform	BTC
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/Orange-Chain/orange-bridge-contract
Commits	a50f9c915a3acfc0f1e1fbb812bc9a8c48d04ba4 ef6924d07355c54413b5e9716bb1ec982766347a

1.2 Files in Scope

The following are the SHA1 hashes of the original reviewed files.

ID	File	SHA-1 Hash
BFR	contracts/BridgeFeeRates.sol	1849acd7308cf624822f59d35db38101ecda015d
BTCL2B	contracts/BTCLayer2Bridge.sol	465e3fb4110e8c8f4c9f824b995c8f1387e3ab9b
ERC2T	contracts/ERC20Token.sol	b359394f90fb6bd6c15ed887e5e89e3f10280925
ERC2TW	contracts/ERC20TokenWrapped.sol	6e2bc33582606cf071bec25fd5864520203932ac
BTCL2BERC2	contracts/BTCLayer2BridgeERC20.sol	51ccd03f8d0c286c36b266c307240cdfaed6a136

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	4	2	2
Informational	0	0	0
Minor	3	2	1
Medium	1	0	1
Major	0	0	0
Critical	0	0	0

1.4 ScaleBit Audit Breakdown

ScaleBit aims to assess repositories for security-related issues, code quality, and compliance with specifications and best practices. Possible issues our team looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Integer overflow/underflow
- Number of rounding errors
- Unchecked External Call
- Unchecked CALL Return Values
- Functionality Checks
- Reentrancy
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic issues
- Gas usage
- Fallback function usage
- tx.origin authentication
- Replay attacks
- Coding style issues

1.5 Methodology

The security team adopted the **"Testing and Automated Analysis"**, **"Code Review"** and **"Formal Verification"** strategy to perform a complete security test on the code in a way that is closest to the real attack. The main entrance and scope of security testing are stated in the conventions in the "Audit Objective", which can expand to contexts beyond the scope according to the actual testing needs. The main types of this security audit include:

(1) Testing and Automated Analysis

Items to check: state consistency / failure rollback / unit testing / value overflows / parameter verification / unhandled errors / boundary checking / coding specifications.

(2) Code Review

The code scope is illustrated in section 1.2.

(3) Audit Process

- Carry out relevant security tests on the testnet or the mainnet;
- If there are any questions during the audit process, communicate with the code owner in time. The code owners should actively cooperate (this might include providing the latest stable source code, relevant deployment scripts or methods, transaction signature scripts, exchange docking schemes, etc.);
- The necessary information during the audit process will be well documented for both the audit team and the code owner in a timely manner.

2 Summary

This report has been commissioned by Orange to identify any potential issues and vulnerabilities in the source code of the Orange smart contract, as well as any contract dependencies that were not part of an officially recognized library. In this audit, we have utilized various techniques, including manual code review and static analysis, to identify potential vulnerabilities and security issues.

During the audit, we identified 4 issues of varying severity, listed below.

ID	Title	Severity	Status
BTC-1	`Initialize` Could Be Front-Run	Minor	Acknowledged
BTC-2	Use `abi.encode` instead of `abi.encodePacked`	Minor	Fixed
BTC1-1	Single-step Ownership Transfer Can be Dangerous	Medium	Acknowledged
BTC1-2	Lack of Events Emit	Minor	Fixed

3 Participant Process

Here are the relevant actors with their respective abilities within the Orange Smart Contract :

Owner

- The owner can call the `setSuperAdminAddress` function to set `superAdminAddress` .
- The owner can call the `addProposeAdminAddress` / `delProposeAdminAddress` to add or del the propose admin.
- The owner can call the `addERC20TokenWrapped` function to add an new Warpper Token.
- The owner can invoke the `propose` function to create a propose.
- The owner can utilize the `review` function to review and execute a proposal.
- The owner can invoke the `pause/unpause` function to control the protocol.

User

- Users can call the `lockNativeToken` function to lock native token.

4 Findings

BTC-1 `Initialize` Could Be Front-Run

Severity: Minor

Status: Acknowledged

Code Location:

contracts/BTCLayer2BridgeERC20.sol#32;

contracts/BTCLayer2Bridge.sol#152

Descriptions:

In the contract, by calling the `initialize` function to initialize the contracts, there is a potential issue that malicious attackers preemptively call the initialize function to initialize and there is no access control verification for the initialize functions.

Suggestion:

It is suggested that the `initialize` function can be called only by privileged addresses or in the same transaction immediately after the contract is created to avoid being maliciously called by the attacker.

Resolution:

The client response deployment and initialization will be in the same transaction.

BTC-2 Use `abi.encode` instead of `abi.encodePacked`

Severity: Minor

Status: Fixed

Code Location:

contracts/BTCLayer2BridgeERC20.sol#43

Descriptions:

Use `abi.encode()` instead which will pad items to 32 bytes, which will prevent hash collisions (e.g. `abi.encodePacked(0x123,0x456)` => `0x123456` => `abi.encodePacked(0x1,0x23456)` , but `abi.encode(0x123,0x456)` => `0x0...1230...456`). Unless there is a compelling reason, `abi.encode` should be preferred.

Suggestion:

It is recommended to use `abi.encode` as preferred.

BTC1-1 Single-step Ownership Transfer Can be Dangerous

Severity: Medium

Status: Acknowledged

Code Location:

contracts/BTCLayer2Bridge.sol#157

Descriptions:

Single-step ownership transfer means that if a wrong address was passed when transferring ownership or admin rights it can mean that role is lost forever. If the admin permissions are given to the wrong address within this function, it will cause irreparable damage to the contract.

Suggestion:

It is recommended to use a two-step ownership transfer pattern for `superAdminAddress`.

Resolution:

The client response will use multiple signatures to avoid this problem.

BTC1-2 Lack of Events Emit

Severity: Minor

Status: Fixed

Code Location:

contracts/BTCLayer2Bridge.sol#348

Descriptions:

The contract lacks appropriate events for monitoring sensitive operations, which could make it difficult to track sensitive actions or detect potential issues. For example, the `setChainIdSupport` function.

Suggestion:

It is recommended to emit events for those important functions.

Appendix 1

Issue Level

- **Informational** issues are often recommendations to improve the style of the code or to optimize code that does not affect the overall functionality.
- **Minor** issues are general suggestions relevant to best practices and readability. They don't post any direct risk. Developers are encouraged to fix them.
- **Medium** issues are non-exploitable problems and not security vulnerabilities. They should be fixed unless there is a specific reason not to.
- **Major** issues are security vulnerabilities. They put a portion of users' sensitive information at risk, and often are not directly exploitable. All major issues should be fixed.
- **Critical** issues are directly exploitable security vulnerabilities. They put users' sensitive information at risk. All critical issues should be fixed.

Issue Status

- **Fixed:** The issue has been resolved.
- **Partially Fixed:** The issue has been partially resolved.
- **Acknowledged:** The issue has been acknowledged by the code owner, and the code owner confirms it's as designed, and decides to keep it.

Appendix 2

Disclaimer

This report is based on the scope of materials and documents provided, with a limited review at the time provided. Results may not be complete and do not include all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your own risk. A report does not imply an endorsement of any particular project or team, nor does it guarantee its security. These reports should not be relied upon in any way by any third party, including for the purpose of making any decision to buy or sell products, services, or any other assets. TO THE FULLEST EXTENT PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS REPORT, ITS CONTENT, RELATED SERVICES AND PRODUCTS, AND YOUR USE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NOT INFRINGEMENT.

SCALEBIT VERIFIED