Protocol Baobao

Smart Contract Audit Report

Document Info

Project Name	Baobao
Project Website	https://blockbao.io/
Audit Period	15.02.2024 - 18.02.2024
Audit Result	Passed
Report Prepared By	Roy Zhang
Changelog	18.02.2024 - Release Report

Audit Scope

Project Repo	https://github.com/*PRIVATEREPO*/redPacket
Audit Commit	64344c94981721ecd37c3adf4b4f03a1b3d64a0d

├─redPacket
│ InscriptionRedPacket.sol @
│ RedPacket.sol
│ RedPacketStorage.sol

Summary

Protocol Baobao Baobao is an early Telegram web3 ecosystem that aims to redefine crypto promotion by offering a comprehensive crypto red packet tool. With Baobao, users can effortlessly send a variety of crypto red packets on Telegram, including cross-chain inscription tokens and NFTs, without any gas fees. The platform allows for easy distribution of red packets in Telegram chats, amplifying their reach and user interaction. Additionally, red packets can serve as a powerful community booster, enhancing interactions and involvement after token launches. Baobao also offers direct in-app trading of cryptocurrencies within Telegram, eliminating the need for external applications or extensions. Users can further customize the red packets by implementing specific criteria to restrict access and claim only by designated token holders. Overall, Baobao aims to revolutionize crypto promotion and create a fun and engaging experience for users.

After our inspection and auditing according to industry standards, we found NO CRITICAL, HIGH, MEDIUM risk problems. There are two LOW risk issues that need special attention in future operations. Please refer to the summary below and see the Audit Details for implementation details. The contract for this protocol is kept minimal and free from any major security issues.

#	Finding	Risk Level	Comments from Project Team
R1	Uncheck “audience” in JWT which can cause phishing problems.	Low	Risk Accepted. Unused Code.
R2	Leakage of the owner's private key could lead to funds lost.	Low	Risk Accepted. Additional measures will be taken to protect the private key

Audit Detail

ID:	R1	File:	RedPacket.sol	Risk:	Low
Finding:	Inconsistency between comment and implementation				

//RedPacket.sol: Line 10

```
    function createNormalPacket(uint256 amount, uint16 nums, address room) external {
        require(nums <= 10000, "nums must be bwt 1,10000");
```

//ElessarLabs: The uint16 includes 0, but the require check doesn't check 0, which may lead to unintentional behavior.

ID:	R2	File:	InscriptionRedPacket.sol	Risk:	Low
Finding:	Leakage of the owner's private key could lead to funds lost.				

//InscriptionRedPacket.sol: Line 104

```
   function rescue(address token) external onlyOwner {
        if (token == address(0)) {
            Address.sendValue(payable(owner()), address(this).balance);
        } else {
            IERC20Metadata(token).safeTransfer(owner(),
IERC20Metadata(token).balanceOf(address(this)));
        }
    }
```

//ElessarLabs: If hackers gain control on the owner’s private key, they can easily loot funds from the project.

Disclaimer

ElessarLabs issues this report only based on the facts that have happened or existed before the report is issued, and will take the corresponding responsibilities for the report based on these facts. Regarding any unknown vulnerabilities or security incidents that happen or exist after the issue of this report, ElessarLabs cannot verify their security conditions and will not be responsible for them. All of the security audits analysis and other contents in this report are only based on the files and documents provided to ElessarLabs by information providers(hereinafter referred to as "provided documents"). ElessarLabs assumes that the provided documents are not under any of these circumstances, such as being absent, being tampered, being abridged or being concealed. If the information of the provided documents were absent, tampered, abridged, concealed, or did not conform to the reality, ElessarLabs would not be responsible for any of the loss or disadvantages caused by these circumstances. ElessarLabs only performs the appointed security audits for the security condition of this project and issues this report. ElessarLabs is not responsible for the background of this project or any other circumstances.