BEOSIN
Blockchain Security

Cicada

Smart Contract Security Audit

No. 202408151045

Aug 15th, 2024

SECURING BLOCKCHAIN ECOSYSTEM

WWW.BEOSIN.COM

Contents

Summary of Audit Results

After auditing, 3 Medium Risk item was identified in the Cicada project. Specific audit details will be presented in the Findings section. Users should pay attention to the following aspects when interacting with this project:

Medium	Fixed : 3	Acknowledged: 0

- **Project Description:**

1. Basic Token Information

Token name	Cicada finance
Token symbol	ciBTC
Decimals	18
Token type	ERC-20

Table 1 ciBTC token info

2. Business overview

Cicada primarily consists of the CiBTC token contract and the business contracts StakeCiBtc/StakeCiBtc2.

CiBTC is an ERC-20 token. Its implementation adds a mint role to the standard ERC-20, along with the `mintTo` and `burn` functions that can only be called by the mint role. The `mintTo` function allows minting an arbitrary number of tokens to any address, which poses a centralization risk. However, the project team states that Cicada utilizes a Gnosis Safe multisig to hold ownership of its smart contracts.

StakeCiBtc is mainly used for deposit and withdrawal of funds, supporting platform tokens and specified tokens. This contract calls external contracts for fund custody and mints ciBTC tokens as proof. When withdrawing, a withdrawal signature must first be provided, which is signed off-chain by a designated address. If the signature validation is successful, the user can proceed with the withdrawal, and the ciBTC tokens are burned.

StakeCiBtc2 is also used for deposit and withdrawal of funds, but unlike StakeCiBtc, it does not require a signature for withdrawals. Instead, it directly burns ciBTC on-chain and returns the designated asset to the user.

It is important to note that both contracts include the `withdrawTokensSelf` function, which allows the admin to extract all assets from the contract (although the contract is theoretically not meant to hold assets directly), presenting a certain degree of centralization risk. The project team asserts that Cicada utilizes a Gnosis Safe multisig to hold ownership of its smart contracts.

1 Overview

1.1 Project Overview

Project Name	Cicada
Project Language	Solidity
Platform	Merlin Chain
Code base	https://github.com/mineral-devlop/Cicada-contracts
Commit hash	bee560507a481514b2b1be392378870cc98d4720 5b01a00a9bfb0a1b178e651c6ceb26f55404251e ddd65309fd90dc7f12dcfdcc9cab85cfb6ba61ce

1.2 Audit Overview

Audit work duration: Aug 13, 2024 - Aug 15, 2024

Audit team: Beosin Security Team

1.3 Audit Method

The audit methods are as follows:

1. Formal Verification

Formal verification is a technique that uses property-based approaches for testing and verification. Property specifications define a set of rules using Beosin's library of security expert rules. These rules call into the contracts under analysis and make various assertions about their behavior. The rules of the specification play a crucial role in the analysis. If the rule is violated, a concrete test case is provided to demonstrate the violation.

2. Manual Review

Using manual auditing methods, the code is read line by line to identify potential security issues. This ensures that the contract's execution logic aligns with the client's specifications and intentions, thereby safeguarding the accuracy of the contract's business logic.

The manual audit is divided into three groups to cover the entire auditing process:

The Basic Testing Group is primarily responsible for interpreting the project's code and conducting comprehensive functional testing.

The Simulated Attack Group is responsible for analyzing the audited project based on the collected historical audit vulnerability database and security incident attack models. They identify potential attack vectors and collaborate with the Basic Testing Group to conduct simulated attack tests.

The Expert Analysis Group is responsible for analyzing the overall project design, interactions with third parties, and security risks in the on-chain operational environment. They also conduct a review of the entire audit findings.

3. Static Analysis

Static analysis is a method of examining code during compilation or static analysis to detect issues. Beosin-VaaS can detect more than 100 common smart contract vulnerabilities through static analysis, such as reentrancy and block parameter dependency. It allows early and efficient discovery of problems to improve code quality and security.

2 Findings

Index	Risk description	Severity level	Status
Cicada-01	ID not updated causing signature reuse	Medium	Fixed
Cicada-02	Token changes can lead to business failure	Medium	Fixed
Cicada-03	Centralization risk	Medium	Fixed

Finding Details:

[Cicada-01] ID not updated causing signature reuse

Severity Level	Medium
Type	Business Security
Lines	StakeBibtc .sol #L171-201
Description	In the StakeBibtc contract, users need to verify the signature when using the `withdraw` function, and the id ensures that the signature cannot be reused. However, in the actual implementation, the value of withdraw[id] is not updated to true after the signature is used, which means that the requirement(!withdraws[id]) can still pass the verification, allowing the signature to be reused.

```
function withdraw(
    address token,
    uint256 id,
    uint256 amount,
    uint256 assets,
    address user,
    uint deadline,
    bytes memory signature
) public notSupportToken(token) notZero(assets) {
    require(block.timestamp <= deadline, "deadline");
    require(user == msg.sender, "sender not match");
    require(!withdraws[id], "had claimed");
    require(
        verifySign(token, id, assets, amount, user, deadline,
signature),
        "Invalid signature"
    );
    IERC20(ciBTC).safeTransferFrom(user, address(this), assets);
    uint _balance = IERC20(ciBTC).balanceOf(address(this));
    ICiBtc(ciBTC).burn(_balance);
    if (token == address(0)) {
        (bool success, ) = msg.sender.call{value: amount, gas:
10_000}("");
        require(success, "WITHDRAW_FAILED");
    } else {
```

```
        IERC20(token).safeTransfer(user, amount);
    }
    emit Withdrawal(id, user, amount, block.timestamp);
}
```

Recommendation	It is recommended to add the update withdraw[id]=true to prevent signature reuse.
Status	**Fixed.** `withdraws[id] = true;`

[Cicada-02] Token changes can lead to business failure

Severity Level	**Medium**
Type	Business Security
Lines	StakeBibtc2.sol #L107-124
Description	In the StakeCiBtc2 contract, the Collateral token can be modified. This means that the token deposited and the token withdrawn may be different, which could lead to a failure in withdrawal due to insufficient token balance. For example, the user deposits Collateral token A, and the rBTC contract stores token A. If the Collateral token is then changed to token B, when the user calls the withdraw function, the rBTC contract will try to transfer token B. If there are not enough token B in the rBTC contract, the withdrawal will fail.
Recommendation	It is recommended that the project team should consider restricting the modification of collateral tokens based on the project's actual logic.
Status	**Fixed.** The project team has removed the functions related to modifying the collateral tokens.

```
function withdraw(uint256 amount) public nonReentrant notZero(amount)
{
    if (hasRole(CIBTC_STAKER_ROLE, msg.sender)) {
        revert OperationNotAllowed();
    }
    require(
        amount <= IERC20(ciBTC).balanceOf(msg.sender),
        "INSUFFICIENT_ciBTC_BALANCE"
    );
    uint beforeCollateral = collateral.balanceOf(address(this));
    rBTC.withdraw(amount);
    uint afterCollateral = collateral.balanceOf(address(this));
    IERC20(ciBTC).safeTransferFrom(msg.sender, address(this), amount);
    uint _balance = IERC20(ciBTC).balanceOf(address(this));
    ICiBtc(ciBTC).burn(_balance);
    collateral.safeTransfer(msg.sender, afterCollateral -
beforeCollateral);
    emit Withdrawal(msg.sender, amount, block.timestamp);
}
```

[Cicada-03] Centralization risk

Severity Level	Medium
Type	Business Security
Lines	CiBtc.sol #L18, 31-33 StakeBibtc.sol #L87-102
Description	1) In the StakeCiBtc contract, the admin role can call the `withdrawTokensSelf` function to withdraw all the assets, which concentrates too much power and poses a centralization risk. If the private key is lost, it could lead to significant losses.

```
function withdrawTokensSelf(
    address token,
    address to
) external onlyRole(DEFAULT_ADMIN_ROLE) {
    require(to != address(0), "Cannot be zero address");
    if (token == address(0)) {
        (bool success, ) = to.call{value: address(this).balance}("");
        if (!success) {
            revert();
        }
    } else {
        uint256 bal = IERC20(token).balanceOf(address(this));
        IERC20(token).safeTransfer(to, bal);
    }
    emit Withdraw(token, to);
}
```

2) In the CiBtc contract's constructor, 100 million tokens were minted to the msg.sender at once, which concentrates the tokens and poses a centralization risk. If the private key is lost, it could lead to significant losses.

```
constructor(address _admin, address _mintRole) ERC20("Cicada finance",
"ciBTC") {
    if (_admin == address(0) || _mintRole == address(0)) {
        revert InvalidZeroAddress();
    }
    _mint(msg.sender, 10 ** 8 * 1e18);
    _grantRole(MINT_ROLE, _mintRole);
    _grantRole(DEFAULT_ADMIN_ROLE, _admin);
}
```

	3) In the CiBtc contract, the admin role can call the `mintTo` function to mint tokens to any address, which poses a centralization risk. `function mintTo(address to, uint256 amount) external onlyRole(MINT_ROLE) { _mint(to, amount); }`
Recommendation	It is recommended to use a multi-signature wallet to manage the owner permissions of the contract.
Status	**Fixed.** The project owner declares that it will use a gnosis safe multisig to hold ownership of its smart contracts.

3 Appendix

3.1 Vulnerability Assessment Metrics and Status in Smart Contracts

3.1.1 Metrics

In order to objectively assess the severity level of vulnerabilities in blockchain systems, this report provides detailed assessment metrics for security vulnerabilities in smart contracts with reference to CVSS 3.1(Common Vulnerability Scoring System Ver 3.1).

According to the severity level of vulnerability, the vulnerabilities are classified into four levels: "critical", "high", "medium" and "low". It mainly relies on the degree of impact and likelihood of exploitation of the vulnerability, supplemented by other comprehensive factors to determine of the severity level.

Likelihood \ Impact	Severe	High	Medium	Low
Probable	Critical	High	Medium	Low
Possible	High	Medium	Medium	Low
Unlikely	Medium	Medium	Low	Info
Rare	Low	Low	Info	Info

3.1.2 Degree of impact

- **Severe**

Severe impact generally refers to the vulnerability can have a serious impact on the confidentiality, integrity, availability of smart contracts or their economic model, which can cause substantial economic losses to the contract business system, large-scale data disruption, loss of authority management, failure of key functions, loss of credibility, or indirectly affect the operation of other smart contracts associated with it and cause substantial losses, as well as other severe and mostly irreversible harm.

- **High**

High impact generally refers to the vulnerability can have a relatively serious impact on the confidentiality, integrity, availability of the smart contract or its economic model, which can cause a greater economic loss, local functional unavailability, loss of credibility and other impact to the contract business system.

- **Medium**

Medium impact generally refers to the vulnerability can have a relatively minor impact on the confidentiality, integrity, availability of the smart contract or its economic model, which can cause a small amount of economic loss to the contract business system, individual business unavailability and other impact.

- **Low**

Low impact generally refers to the vulnerability can have a minor impact on the smart contract, which can pose certain security threat to the contract business system and needs to be improved.

3.1.3 Likelihood of Exploitation

- **Probable**

Probable likelihood generally means that the cost required to exploit the vulnerability is low, with no special exploitation threshold, and the vulnerability can be triggered consistently.

- **Possible**

Possible likelihood generally means that exploiting such vulnerability requires a certain cost, or there are certain conditions for exploitation, and the vulnerability is not easily and consistently triggered.

- **Unlikely**

Unlikely likelihood generally means that the vulnerability requires a high cost, or the exploitation conditions are very demanding and the vulnerability is highly difficult to trigger.

- **Rare**

Rare likelihood generally means that the vulnerability requires an extremely high cost or the conditions for exploitation are extremely difficult to achieve.

3.1.4 Fix Results Status

Status	Description
Fixed	The project party fully fixes a vulnerability.
Partially Fixed	The project party did not fully fix the issue, but only mitigated the issue.
Acknowledged	The project party confirms and chooses to ignore the issue.

3.2 Audit Categories

No.	Categories	Subitems
1	Coding Conventions	Compiler Version Security
		Deprecated Items
		Redundant Code
		require/assert Usage
		Gas Consumption
2	General Vulnerability	Integer Overflow/Underflow
		Reentrancy
		Pseudo-random Number Generator (PRNG)
		Transaction-Ordering Dependence
		DoS (Denial of Service)
		Function Call Permissions
		call/delegatecall Security
		Returned Value Security
		tx.origin Usage
		Replay Attack
		Overriding Variables
		Third-party Protocol Interface Consistency
3	Business Security	Business Logics
		Business Implementations
		Manipulable Token Price
		Centralized Asset Control
		Asset Tradability
		Arbitrage Attack

Beosin classified the security issues of smart contracts into three categories: Coding Conventions, General Vulnerability, Business Security. Their specific definitions are as follows:

- **Coding Conventions**

Audit whether smart contracts follow recommended language security coding practices. For example, smart contracts developed in Solidity language should fix the compiler version and do not use deprecated keywords.

- **General Vulnerability**

General Vulnerability include some common vulnerabilities that may appear in smart contract projects. These vulnerabilities are mainly related to the characteristics of the smart contract itself, such as integer overflow/underflow and denial of service attacks.

- **Business Security**

Business security is mainly related to some issues related to the business realized by each project, and has a relatively strong pertinence. For example, whether the lock-up plan in the code match the white paper, or the flash loan attack caused by the incorrect setting of the price acquisition oracle.

*Note that the project may suffer stake losses due to the integrated third-party protocol. This is not something Beosin can control. Business security requires the participation of the project party. The project party and users need to stay vigilant at all times.

3.3 Disclaimer

The Audit Report issued by Beosin is related to the services agreed in the relevant service agreement. The Project Party or the Served Party (hereinafter referred to as the "Served Party") can only be used within the conditions and scope agreed in the service agreement. Other third parties shall not transmit, disclose, quote, rely on or tamper with the Audit Report issued for any purpose.

The Audit Report issued by Beosin is made solely for the code, and any description, expression or wording contained therein shall not be interpreted as affirmation or confirmation of the project, nor shall any warranty or guarantee be given as to the absolute flawlessness of the code analyzed, the code team, the business model or legal compliance.

The Audit Report issued by Beosin is only based on the code provided by the Served Party and the technology currently available to Beosin. However, due to the technical limitations of any organization, and in the event that the code provided by the Served Party is missing information, tampered with, deleted, hidden or subsequently altered, the audit report may still fail to fully enumerate all the risks.

The Audit Report issued by Beosin in no way provides investment advice on any project, nor should it be utilized as investment suggestions of any type. This report represents an extensive evaluation process designed to help our customers improve code quality while mitigating the high risks in blockchain.

3.4 About Beosin

Beosin is the first institution in the world specializing in the construction of blockchain security ecosystem. The core team members are all professors, postdocs, PhDs, and Internet elites from world-renowned academic institutions. Beosin has more than 20 years of research in formal verification technology, trusted computing, mobile security and kernel security, with overseas experience in studying and collaborating in project research at well-known universities. Through the security audit and defense deployment of more than 2,000 smart contracts, over 50 public blockchains and wallets, and nearly 100 exchanges worldwide, Beosin has accumulated rich experience in security attack and defense of the blockchain field, and has developed several security products specifically for blockchain.

BEOSIN
Blockchain Security

Official Website
https://www.beosin.com

Telegram
https://t.me/beosin

Twitter
https://twitter.com/Beosin_com

Email
service@beosin.com