BEOSIN
Blockchain Security

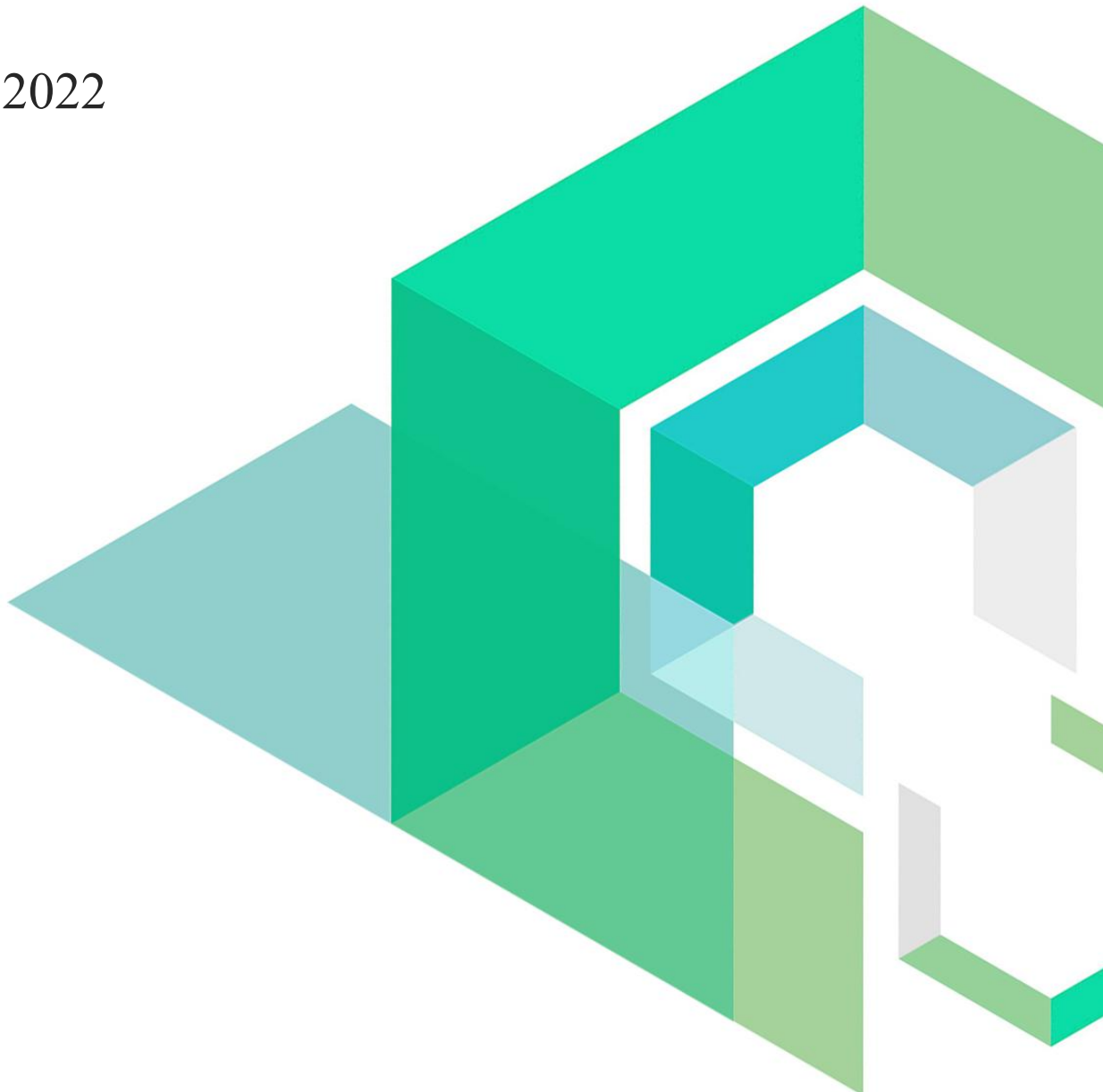
DRAC

Smart Contract Security Audit

V1.0

No. 202208021436

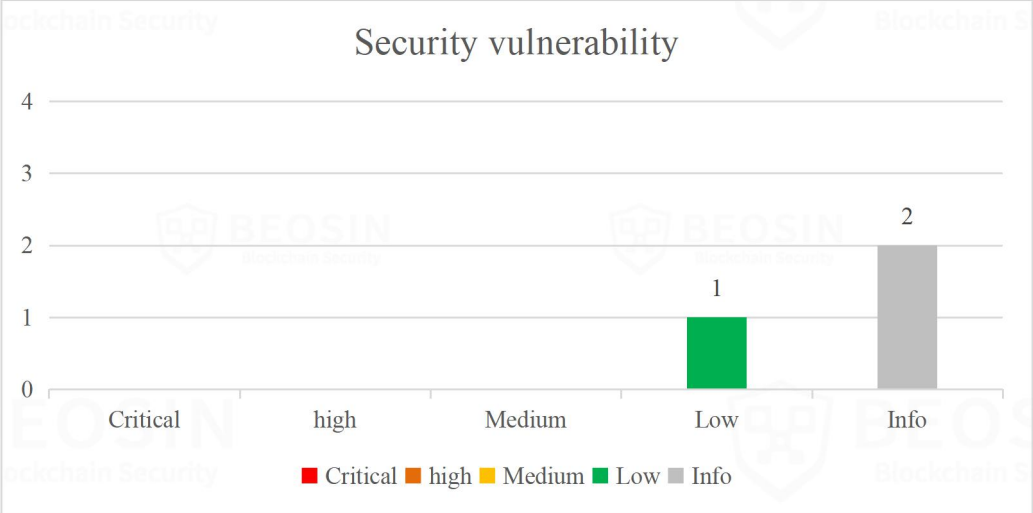
Aug 2nd, 2022



Contents

Summary of audit results

After auditing, 1 Low-risk and 2 Info items were identified in the DRAC project. Specific audit details will be presented in the **Findings section**. Users should pay attention to the following aspects when interacting with this project:



*Notes：

- **Risk Description:**

1. When addLiquidityEnable is false, all users will not only be able to grant router address allowances, but also cannot call the approve function to grant other address allowances.

2. When the token interacts with the pair using the transfer or transferFrom function when the user is not a whitelisted user or when TaxEnable is not enabled, a 2% fee will be incurred.

3. The *transfer* and *transferFrom* functions have inconsistent fee processing logic. When the user interacts with the pair using the *transfer* function, 2% of the amount will be burned. When the user interacts with the pair using the *transferFrom* function, 2% of the amount will be sent to the MarketAddress address.

4. The contract has no mint function, all Pre-mint tokens are held by the _owner.

- **Project Description:**

1. Basic Token Information

Token name	DRAC Token
Token symbol	DRAC
Decimals	18
Pre-mint	100 million
Total supply	100 million
Token type	BEP-20

2. Business overview

This project is a token contract. When the contract is initialized, a pair of WETH and this token will be added. When the token is not a whitelisted user or when TaxEnable is not enabled, using transfer and transferFrom to interact with pair will incur a 2% fee.

1 Overview

1.1 Project Overview

Project Name	DRAC
Platform	BNB Chain
Contract Address	0x123458C167a371250d325Bd8B1ffF12C8AF692A7

1.2 Audit Overview

Audit work duration：Aug 1, 2022 – Aug 2, 2022

Audit methods: Formal Verification, Static Analysis, Typical Case Testing and Manual Review.

Audit team: Beosin Technology Co. Ltd.

2 Findings

Index	Risk description	Severity level	Status
DRAC-1	Repeated addition of invalid index	Low	Acknowledged
DRAC-2	Centralization risk	Info	Acknowledged
DRAC-3	The native token transferred by mistake will be locked	Info	Acknowledged

Risk Details Description:

1. DRAC-1 is not fixed, and repeated addition of the whitelist will result in repeated indexing.

2. DRAC-2 is not fixed, but there is no effect on the project.

3. DRAC-3 is not fixed, and if the native token is transferred to the contract, it will be locked in the contract.

[DRAC-1] Repeated addition of invalid index

Severity Level	**Low**
Type	Business Security
Lines	DRAC_Mainnet.sol #L81-82
Description	*addWhiteList* function does not judge whether the address has been added to the whitelist, which will cause the whitelist to be removed when the same address is added twice, and the WhiteLists ledger will push the address twice.

```
80      function addWhiteList(address account) external onlyOwner{
81          WhiteList[account] = !WhiteList[account];
82          WhiteLists.push(account);
83      }
```

Figure 1 Source code of *addWhiteList* function (unfixed)

Recommendations	It is recommended to *addWhiteList* function to determine whether the address has been added to the whitelist, and add a function to remove an account in the whitelist.
Status	**Acknowledged.**

[DRAC-2] Centralization risk

Severity Level	**Info**
Type	Business Security
Lines	DRAC_Mainnet.sol #L58
Description	All Pre-mint tokens in this contract are on the _owner address, and there is a risk of centralization.

```
53      constructor() {
54          _name = "DRAC Token";
55          _symbol = "DRAC";
56          _owner = address(0x8c4c81CED567533BA2909a6952395FA5367Aa38F);
57          MarketAddress = address(0xF3412cFEf2C0140C72cDc8E2F7C76E305fFC11FE);
58          _mint(_owner, 1 * 1e8 * 1e18);
59          IPancakeSwapV2Router01 _uniswapV2Router = IPancakeSwapV2Router01(0x10ED43C718714eb63d5aA57B78B54704E256024E);
60          uniswapV2Pair = IPancakeSwapV2Factory(_uniswapV2Router.factory())
61              .createPair(address(this), _uniswapV2Router.WETH());
62
63          uniswapV2Router = _uniswapV2Router;
64          Pair[address(uniswapV2Pair)] = true;
65          _approve(_owner, address(uniswapV2Router), type(uint256).max);
66      }
```

Figure 2 Source code of constructor

Recommendations	It is recommended to keep the private key by multi-signature or use DAO for governance.
Status	**Acknowledged.**

[DRAC-3] The native token transferred by mistake will be locked

Severity Level	**Info**
Type	Business Security
Lines	DRAC_Mainnet.sol # L287
Description	There is a *receive* function in the contract, but there is no function designed to withdraw the contract's native token, which will cause the native token entered into the contract by mistake to be unable to be withdrawn.

```
285     }
286
287     receive() external payable {}
288
289 }
```

Figure 3 Source code of *receive* function

Recommendations	It is recommended to add a function that can withdraw the native tokens in the contract.
Status	**Acknowledged.**

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	High	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.

3.1.4 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.

3.1.5 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

Affiliated to BEOSIN Technology Pte. Ltd., 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/+dD8Bnqd133RmNWNl

Twitter

https://twitter.com/Beosin_com

Email

Contact@beosin.com