BINENET

Smart Contract Audit Report

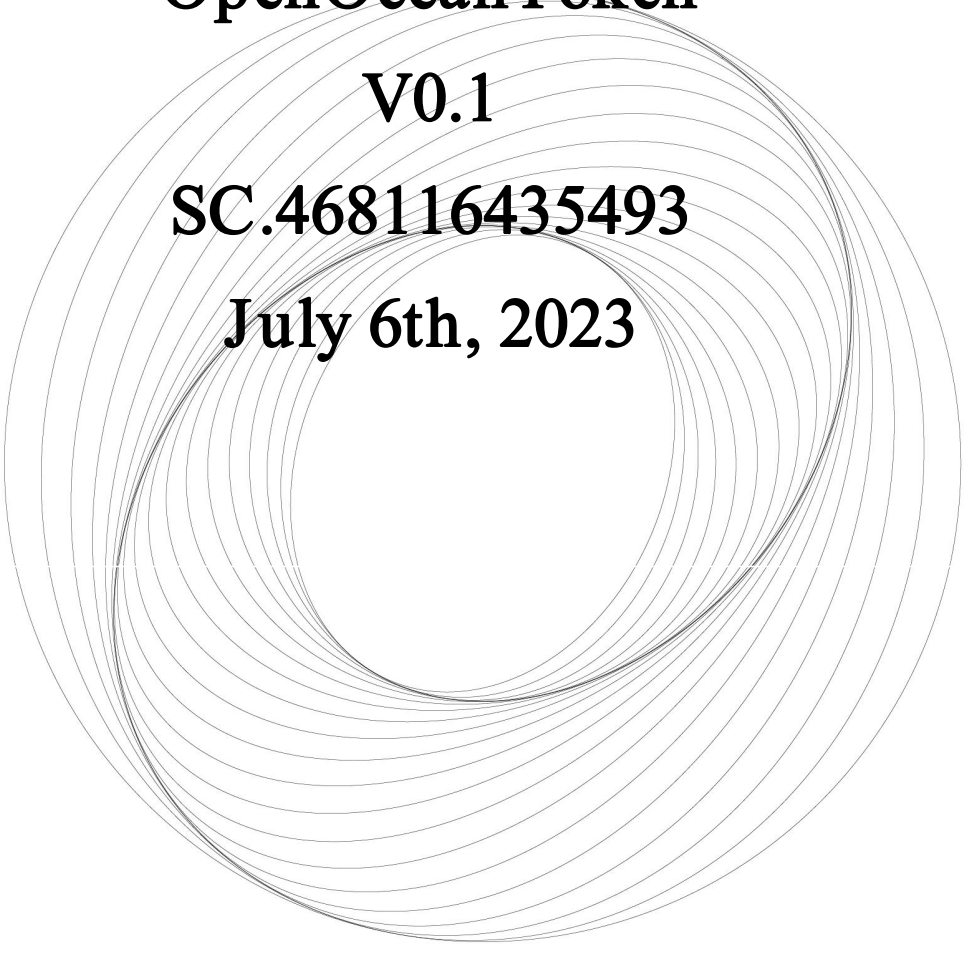
BNBChain

OpenOceanToken

V0.1

SC.468116435493

July 6th, 2023



Contents

1 Report Overview

Binenet security team have audited the OpenOceanToken, 0 risks was identified in OpenOceanToken. users should pay attention to the following aspects when interacting with this project.

Contract Code	Function	Security Level	Status	Fix Result
---	---	---	---	---

*Risk Description: ---

2 Asset Management Security Assessment

Asset Type	Function	Security Level
User Mortgage Token Assets	---	---
Users Mortgage Platform Currency Assets	---	---

Description:Check the management security of digital currency assets transferred by users in the contract business logic. Observe whether there are security risks that may cause the loss of customer funds, such as the digital currency assets transferred into the contract are incorrectly recorded or transferred out by mistake.

3 Audit Overview

3.1 Project Information

OpenOcean is the leading DEX aggregator, integrating the most liquidity sources across a wide range of blockchains into one seamless trading interface, to bring users one-stop trading solution!

This is a reference implementation of the OpenOceanToken standard.

3.2 Audit Information

Project Name	OpenOceanToken
Platform	BNBChain
Audit Scope	OpenOceanToken.sol[Proxy]#https://bscscan.com/address/0x8ea5219a16c2dbf1d6335a6aa0c6bd45c50347c5#code OpenOceanTokenImpl.sol[Logic]#https://bscscan.com/address/0xd332534c9fd5d28846b012027965d1f1d602d36b#code
Website	https://openocean.finance/

3.3 External Visibility Analysis

Function	Visibility	State Change	Modifier	Payable	Description
approve	public	true	---	---	---
burn	public	true	---	---	---
burnFrom	public	true	---	---	---
decreaseAllowance	public	true	---	---	---
increaseAllowance	public	true	---	---	---

initialize	public	true	initializer	---	---
permit	public	true	---	---	finding 4.1
renounceOwnership	public	true	onlyOwner	---	waive contract ownership
transfer	public	true	---	---	---
transferFrom	public	true	---	---	---
transferOwnership	public	true	onlyOwner	---	---

3.4 Audit Process

Audit time: 2023.7.5- 2023.7.6

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

Audit team: Binenet Security Team.

4 Security Finding Details

4.1 Permit for approve

Severity Level : Remind

Lines : OpenOceanTokenImpl.sol # L1963

Description: The permit design can be signed offline, and the signature information can be submitted to the chain during the execution of the received transfer transaction, allowing authorization and transfer to be completed in one transaction. At the same time, transfer transactions can also be submitted by the recipient (or other third parties), which avoids the need for users (owners of ERC20) to rely on ETH, but there are also potential risks, such as users visiting phishing websites and signing malicious authorized signatures, which can lead to token losses. Users should be careful.

```
1960    /**
1961     * @dev See {IERC20Permit-permit}.
1962     */
1963    function permit(
1964        address owner,
1965        address spender,
1966        uint256 value,
1967        uint256 deadline,
1968        uint8 v,
1969        bytes32 r,
1970        bytes32 s
1971    ) public virtual override {
1972        require(block.timestamp <= deadline, "ERC20Permit: expired deadline");
1973
1974        bytes32 structHash = keccak256(abi.encode(_PERMIT_TYPEHASH, owner, spender, value, _useNonce(owner), deadline));
1975
1976        bytes32 hash = _hashTypedDataV4(structHash);
1977
1978        address signer = ECDSAUpgradeable.recover(hash, v, r, s);
1979        require(signer == owner, "ERC20Permit: invalid signature");
1980
1981        _approve(owner, spender, value);
1982    }
```

Recommendations: Before interacting with this function, ensure that the authorization spender and value are known.

Status : Audited.

Fix Result: ---

5 Audit Categories

Categories	Subitems
Business Security	Transfer token function
	Mint token and burn token vulnerability
	Contract logic function
	Mining pool deposit and withdrawal function
	Reasonableness of agreement amendment
	Functional design
	Dos caused by time
	Insecure oracles and their design
	Deployer private key leak hazard
General Vulnerability	Compiler version security
	Redundant code
	Use of safemath library
	Not recommended encoding
	Use require/assert mistakely
	Fallback function safety
	tx.origin authentication
	Owner permission control
	Gas consumption detection
	Call injection attack
	Low-level function safety
	Additional token vulnerabilities
	Access control
	Numeric overflow detection
	Arithmetic precision error
	Misuse of random number detection
	Unsafe external call
	Variable override
	Uninitialized storage pointer

	Return value call validation
	Transaction order dependent detection
	Timestamp dependent attack
	Denial of service attack detection
	Fake recharge vulnerability detection
	Reentrancy Attack Detection
	Replay attack detection
	Reordering attack detection

6 Explanation Of Vulnerability Rating

Vulnerability Rating	Rating Description
High Risk Vulnerabilities	Vulnerabilities that can directly cause the loss of token contracts or user funds, such as: overflow、reentrancy 、false recharge， which can cause the value of tokens to be zeroed, or causing false exchanges to lose tokens, or causing losing ETH or tokens, etc; Vulnerabilities that can cause loss of ownership of token contracts, such as: access control flaws of key functions, call injection leading to access control bypass of key functions, etc; Vulnerabilities that can cause token contracts to fail to work properly, such as: denial of service vulnerabilities caused by sending ETH to malicious addresses, and denial of service vulnerabilities caused by gas exhaustion;
Medium Risk Vulnerability	High-risk vulnerabilities that require specific addresses to be triggered, such as overflow that can only be triggered by token contract owners; access control flaws of non-critical functions, logic design flaws that cannot cause direct financial losses, etc;
Low Risk Vulnerability	Vulnerabilities that are difficult to be triggered, vulnerabilities that cause limited harm after triggering, such as overflow vulnerabilities that require a large amount of ETH or tokens to be triggered, vulnerabilities that the attacker cannot directly profit after triggering overflow, and transaction sequence-dependent risks triggered by specifying high gas wait;

7 Statement

Binenet only issues this report based on the facts that have occurred or existed before the issue of this report, and assumes corresponding responsibilities for it. For the facts that occurred or existed after the issuance, we cannot judge the security status of the smart contract , and we will not be responsible for it.

This report does not include external contract calls , new types of attacks that may appear in the future, and contract upgrades or tampered codes (with the development of the project side, smart contracts may add new pools, new functional modules, new external contract calls, etc.), does not include front-end security and server security.

The documents and materials provided to us by the information provider as of the date of this report.

Binenet assumes that there is no missing, tampered, deleted or concealed information provided. If the information provided is missing, tampered, deleted, concealed or reflected inconsistent with the actual situation, Binenet shall not be liable for any losses and adverse effects resulting therefrom.

8 About Binenet

Founded in June 2021, Binenet is a dedicated and pure blockchain security company, focusing on accurate, efficient and intelligent blockchain threat detection and response. Committed to providing users with professional products and dedicated services in the field of blockchain security. Business functions cover penetration testing, code auditing, emergency response, on-chain data monitoring, AML anti-money laundering, etc., covering all aspects of blockchain ecosystem security.

Official Website
https://binenet.com

Telegram
https://t.me/binenetxyz

Twitter
https://twitter.com/binenetxyz

E-mail
team@binenet.com