RD AUDITORS

Wizarre, Smart Contract, Code Review and Security Analysis Report

Customer: Wizarre
Prepared on: 16th June 2022
Platform: BSC
Language: Solidity

rdauditors.com

Table of Contents

Disclaimer

This document may contain confidential information about its systems and intellectual property of the customer as well as information about potential vulnerabilities and methods of their exploitation.

The report containing confidential information can be used internally by the customer or it can be disclosed publicly after all vulnerabilities are fixed - upon the decision of the customer.

Document

Name	Smart Contract Code Review and Security Analysis Report of Wizarre
Platform	BSC / Solidity
File 1	Wizarre.sol
MD5 hash	5BFA36EDDEFE783F4A9C6C920E93A4D1
SHA256 hash	E4177C729CBEB1232D929EB8A817510C6BD7B5962A905A57874E92AB255B00C3
Date	16/06/2022

Introduction

RD Auditors (Consultant) were contracted by Wizarre (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report represents the findings of the security assessment of the customer`s smart contract and its code review conducted between 10th - 16th June 2022.

This contract consists of one file.

Project Scope

The scope of the project is a smart contract. We have scanned this smart contract for commonly known and more specific vulnerabilities, below are those considered (the full list includes but is not limited to):

- Reentrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with (Unexpected) Throw
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Byte array vulnerabilities
- Style guide violation
- Transfer forwards all gas
- ERC20 API violation
- Malicious libraries
- Compiler version not fixed
- Unchecked external call - Unchecked math
- Unsafe type inference
- Implicit visibility level

Executive Summary

According to the assessment, the customer's solidity smart contract is now **Well-Secured.**

Automated checks are with smartDec, Mythril, Slither and remix IDE. All issues were performed by our team, which included the analysis of code functionality, the manual audit found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the audit overview section. The general overview is presented in the AS-IS section and all issues found are located in the audit overview section.

We found the following;

Total Issues	0
Critical	0
High	0
Medium	0
Low	0
Very Low	0

Code Quality

The libraries within this smart contract are part of a logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned to a specific address and its properties/methods can be reused many times by other contracts.

The Wizarre team has not provided scenario and unit test scripts, which helped to determine the integrity of the code in an automated way.

Documentation

The hash of that file is mentioned in the table. As mentioned above, It's recommended to write comments in the smart contract code, so anyone can quickly understand the programming flow as well as complex code logic.

Comments are very helpful in understanding the overall architecture of the protocol. It also provides a clear overview of the system components, including helpful details, like the lifetime of the background script.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure. Those were based on well known industry standard open source projects and even core code blocks that are written well and systematically.

AS-IS Overview

SummonWizard.sol

File And Function Level Report

File 1: SummonWizard.sol

Contract: SummonWizard

Import: SafeERC20, AccessControl, Pausable

Inherit: AccessControl, Pausable

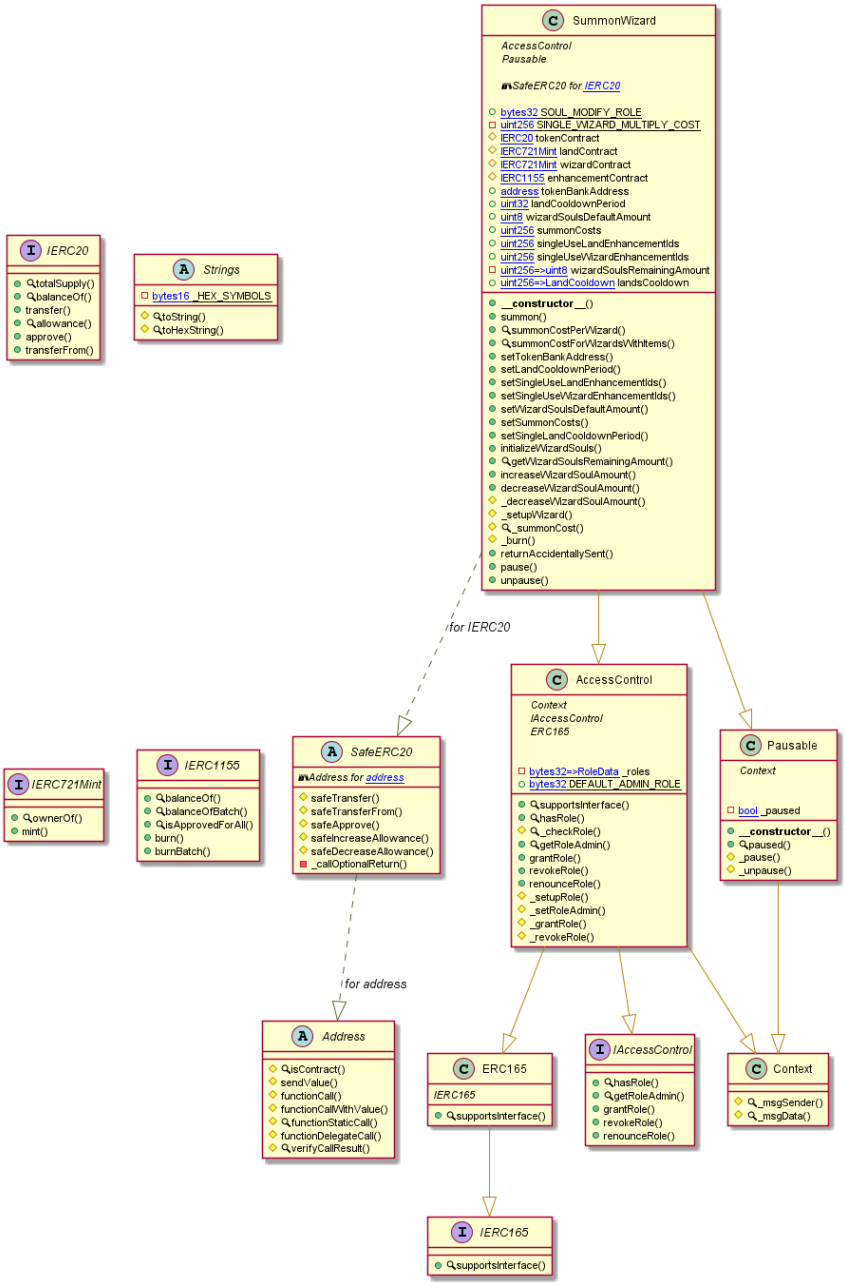
Observation: Passed

Test Report: Passed

Sl.	Function	Type	Observation	Test Report	Conclusion	Score
1	summon	write	Passed	All Passed	No Issue	Passed
2	summonCostPerWizard	write	Passed	All Passed	No Issue	Passed
3	summonCostForWizardsWithItems	write	Passed	All Passed	No Issue	Passed
4	setTokenBankAddress	write	Passed	All Passed	No Issue	Passed
5	setLandCooldownPeriod	write	Passed	All Passed	No Issue	Passed
6	setSingleUseLandEnhancementIds	write	Passed	All Passed	No Issue	Passed
7	setSingleUseWizardEnhancementIds	write	Passed	All Passed	No Issue	Passed

8	setWizardSoulsDefaultAmount	write	Passed	All Passed	No Issue	Passed
9	setSummonCosts	write	Passed	All Passed	No Issue	Passed
10	setSingleLandCooldownPeriod	write	Passed	All Passed	No Issue	Passed
11	initializeWizardSouls	write	Passed	All Passed	No Issue	Passed
12	getWizardSoulsRemainingAmount	read	Passed	All Passed	No Issue	Passed
13	increaseWizardSoulAmount	write	Passed	All Passed	No Issue	Passed
14	decreaseWizardSoulAmount	write	Passed	All Passed	No Issue	Passed
15	_decreaseWizardSoulAmount	write	Passed	All Passed	No Issue	Passed
16	_setupWizard	write	Passed	All Passed	No Issue	Passed
17	_summonCost	read	Passed	All Passed	No Issue	Passed
18	returnAccidentallySent	write	Passed	All Passed	No Issue	Passed
19	pause	write	Passed	All Passed	No Issue	Passed
20	unpause	write	Passed	All Passed	No Issue	Passed

Code Flow Diagram - Wizarre



Code Flow Diagram - Slither Results Log

```
        - SummonWizard.setSingleLandCooldownPeriod(uint256,uint32) (SummonWizard.sol#1197-1201)
        - SummonWizard.setSingleUseLandEnhancementIds(uint256[]) (SummonWizard.sol#1169-1174)
        - SummonWizard.setSingleUseWizardEnhancementIds(uint256[]) (SummonWizard.sol#1176-1181)
        - SummonWizard.setSummonCosts(uint256[]) (SummonWizard.sol#1187-1195)
        - SummonWizard.setTokenBankAddress(address) (SummonWizard.sol#1161-1163)
        - SummonWizard.setWizardSoulsDefaultAmount(uint8) (SummonWizard.sol#1183-1185)
        - SummonWizard.summonCostForWizardsWithItems(uint256[],uint256[]) (SummonWizard.sol#1136-1159)
        - AccessControl.supportsInterface(bytes4) (SummonWizard.sol#735-737)
        - SummonWizard.unpause() (SummonWizard.sol#1318-1320)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unimplemented-functions
INFO:Detectors:
AccessControl._roles (SummonWizard.sol#713) is never used in SummonWizard (SummonWizard.sol#979-1321)
SummonWizard.SINGLE_WIZARD_MULTIPLY_COST (SummonWizard.sol#983) is never used in SummonWizard (SummonWizard.sol#979-1321)
SummonWizard.wizardSoulsRemainingAmount (SummonWizard.sol#996) is never used in SummonWizard (SummonWizard.sol#979-1321)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variables
INFO:Detectors:
SummonWizard.landCooldownPeriod (SummonWizard.sol#991) should be constant
SummonWizard.wizardSoulsDefaultAmount (SummonWizard.sol#992) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Detectors:
grantRole(bytes32,address) should be declared external:
        - AccessControl.grantRole(bytes32,address) (SummonWizard.sol#788-790)
revokeRole(bytes32,address) should be declared external:
        - AccessControl.revokeRole(bytes32,address) (SummonWizard.sol#801-803)
renounceRole(bytes32,address) should be declared external:
        - AccessControl.renounceRole(bytes32,address) (SummonWizard.sol#819-823)
pause() should be declared external:
        - SummonWizard.pause() (SummonWizard.sol#1314-1316)
unpause() should be declared external:
        - SummonWizard.unpause() (SummonWizard.sol#1318-1320)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:SummonWizard.sol analyzed (13 contracts with 75 detectors), 62 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

```
INFO:Detectors:
SummonWizard.summon(uint256[],uint256[],uint256[]) (SummonWizard.sol#1032-1109) has external calls inside a loop: require(bool,
string)(_msgSender() == wizardContract.ownerOf(_wizardIds[_i]),USER_IS_NOT_WIZARD_OWNER) (SummonWizard.sol#1091)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation/#calls-inside-a-loop
INFO:Detectors:
Reentrancy in SummonWizard.summon(uint256[],uint256[],uint256[]) (SummonWizard.sol#1032-1109):
        External calls:
        - tokenContract.transferFrom(_msgSender(),tokenBankAddress,_costSum) (SummonWizard.sol#1096)
        - _newWizardId = wizardContract.mint(_msgSender()) (SummonWizard.sol#1104)
        Event emitted after the call(s):
        - Summoned(_msgSender(),_newWizardId,_landIds,_wizardIds,_ingredientIds,_costSum) (SummonWizard.sol#1106)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
SummonWizard.summon(uint256[],uint256[],uint256[]) (SummonWizard.sol#1032-1109) uses timestamp for comparisons
        Dangerous comparisons:
        - require(bool,string)((landsCooldown[_landIds[0]].start + landsCooldown[_landIds[0]].period) <= uint32(block.timestamp
),LAND_DURING_COOLDOWN) (SummonWizard.sol#1079)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Address.verifyCallResult(bool,bytes,string) (SummonWizard.sol#290-310) uses assembly
        - INLINE ASM (SummonWizard.sol#302-305)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
Different versions of Solidity is used:
        - Version used: ['^0.8.0', '^0.8.1', '^0.8.4']
        - ^0.8.4 (SummonWizard.sol#8)
        - ^0.8.1 (SummonWizard.sol#93)
        - ^0.8.0 (SummonWizard.sol#318)
        - ^0.8.0 (SummonWizard.sol#418)
        - ^0.8.0 (SummonWizard.sol#509)
        - ^0.8.0 (SummonWizard.sol#536)
        - ^0.8.0 (SummonWizard.sol#606)
        - ^0.8.0 (SummonWizard.sol#634)
```

Solidity Static Analysis

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.

more

Pos: 1103:54:

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in SummonWizard.summon(uint256[],uint256[],uint256[]): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.

more

Pos: 1053:4:

Security

Delete dynamic array:

The "delete" operation when applied to a dynamically sized array in Solidity generates code to delete each of the elements contained. If the array is large, this operation can surpass the block gas limit and raise an OOG exception. Also nested dynamically sized objects can produce the same results.

more

Pos: 1209:8:

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to lost tokens etc.
High	High level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g. public access to crucial functions.
Medium	Medium level vulnerabilities are important to fix; however, they cannot lead to lost tokens.
Low	Low level vulnerabilities are most related to outdated, unused etc. These code snippets cannot have a significant impact on execution.
Lowest Code Style/ Best Practice	Lowest level vulnerabilities, code style violations and information statements cannot affect smart contract execution and can be ignored.

Audit Findings

Critical:

No critical severity vulnerabilities were found.

High:

No high severity vulnerabilities were found.

Medium:

No medium severity vulnerabilities were found.

Low:

No low severity vulnerabilities were found.

Very Low:

No very low severity vulnerabilities were found.

Discussion

Please check these loop upper limits before deploying to the mainnet. In your logic you are comparing two values to break out of the loop so if the comparison never matches then this loop will run until the element reaches its last index. There is a possibility of failure.

```
function setSingleUseWizardEnhancementIds(uint256[] calldata _ids) external onlyRole(DEFAULT_ADMIN_ROLE) {
    delete singleUseWizardEnhancementIds;
    for (uint256 i = 0; i < _ids.length; i++) {
        singleUseWizardEnhancementIds.push(_ids[i]);
    }
}
```

```
    uint256 _i;
    uint256 _j;
    int256 _wizardNftAmount = 2;
    for (_i = 0; _i < _ingredientIds.length; _i++) {
        for (_j = 0; _j < singleUseWizardEnhancementIds.length; _j++) {
            if (_ingredientIds[_i] == singleUseWizardEnhancementIds[_j]) {
                _wizardNftAmount--;
                break;
            }
        }
    }
```

```
function setSingleUseLandEnhancementIds(uint256[] calldata _ids) external onlyRole(DEFAULT_ADMIN_ROLE) {
    delete singleUseLandEnhancementIds;
    for (uint256 i = 0; i < _ids.length; i++) {
        singleUseLandEnhancementIds.push(_ids[i]);
    }
}
```

```
    // Check Ingredients
    for (_i = 0; _i < _ingredientIds.length; _i++) {
        // If single-land given then reduce amount of required wizards
        for (_j = 0; _j < singleUseLandEnhancementIds.length; _j++) {
            if (_ingredientIds[_i] == singleUseLandEnhancementIds[_j]) {
                _landNftAmount--;
                break;
            }
        }

        // If single-wizard given then reduce amount of required wizards
        for (_j = 0; _j < singleUseWizardEnhancementIds.length; _j++) {
            if (_ingredientIds[_i] == singleUseWizardEnhancementIds[_j]) {
                _wizardNftAmount--;
                break;
            }
        }
    }
```

Here you can adapt your logic to avoid loops, you can use _ingredientIds length to set _burnValues instead of iterating the loop to set the values.

```
function _burn(uint256[] calldata _ingredientIds) internal {
    uint256[] memory _burnValues = new uint256[](_ingredientIds.length);
    uint256 _i;
    for (_i = 0; _i < _ingredientIds.length; _i++) {
        _burnValues[_i] = 1;
    }
    enhancementContract.burnBatch(_msgSender(), _ingredientIds, _burnValues);
}
```

Conclusion

We were given a contract file and have used all possible tests based on the given object. So it is ready to go for production. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

The security state of the reviewed contract is “**Well-Secured**”.

Note For Contract Users

Technical auditing does not guarantee the project's ethical side.

Please do your due diligence before investing. Our audit report is never an investment advice.

This function gives the owner privileges to transfer all the tokens from the contract.

```
function returnAccidentallySent(IERC20 _tokenToSent) external onlyRole(DEFAULT_ADMIN_ROLE) {
    uint256 _amount = _tokenToSent._burnbalanceOf(address(this));
    _tokenToSent.safeTransfer(_msgSender(), _amount);
}
```

This function gives the owner privileges to pause or unpause the contract.

```
function pause() public onlyRole(DEFAULT_ADMIN_ROLE) {
    _pause();
}

function unpause() public onlyRole(DEFAULT_ADMIN_ROLE) {
    _unpause();
}
```

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyse the feasibility of an attack in a live system.

Suggested Solutions

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinised by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

RD Auditors Disclaimer

The smart contracts given for audit have been analysed in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

Because the total number of test cases are unlimited, the audit makes no statements or warranties on the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only - we recommend proceeding with several independent audits and a public bug bounty program to ensure security of smart contracts.

Technical Disclaimer

Smart contracts are deployed and executed on the blockchain. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can’t guarantee explicit security of the audited smart contracts.

Email: info@rdauditors.com

Website: www.rdauditors.com