

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



This document may contain confidential information about IT systems and the 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 a decision of the Customer.

Document

Name	Smart Contract Code Review and Security Analysis Report for Mozart Finance - Second Review
Approved by	Andrew Matiukhin CTO Hacken OU
Type	BEP20 Governance Token, LP Staking
Platform	Binance Smart Chain / Solidity
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Deployed contracts	https://bscscan.com/address/0x2f619a1270226fd8ed3df82f0c1e0cd90804346d#code https://bscscan.com/address/0x254c3233c162cde86f1b7a91ac801b780f79d40d#code
Timeline	15 MAY 2021 - 8 JUNE 2021
Changelog	18 MAY 2021 - INITIAL AUDIT 8 JUNE 2021 - SECOND REVIEW



Table of contents

Introduction	4
Scope	4
Executive Summary	6
Severity Definitions	8
Audit overview	9
Conclusion	11
Disclaimers	12

Introduction

Hacken OÜ (Consultant) was contracted by Mozart Finance (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on May 18th, 2021.

Scope

The scope of the project is the smart contracts deployed in the Binance Smart Chain mainnet:

<https://bscscan.com/address/0x2f619a1270226fD8ed3Df82f0C1e0cd90804346d#code>
<https://bscscan.com/address/0x254c3233c162cde86f1b7a91ac801b780f79d40d#code>

We have scanned these smart contracts for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that are considered:

Category	Check Item
Code review	<ul style="list-style-type: none">▪ Reentrancy▪ Ownership Takeover▪ Timestamp Dependence▪ Gas Limit and Loops▪ DoS with (Unexpected) Throw▪ DoS with Block Gas Limit▪ Transaction-Ordering Dependence▪ Style guide violation▪ Costly Loop▪ ERC20 API violation▪ Unchecked external call▪ Unchecked math▪ Unsafe type inference▪ Implicit visibility level▪ Deployment Consistency▪ Repository Consistency▪ Data Consistency

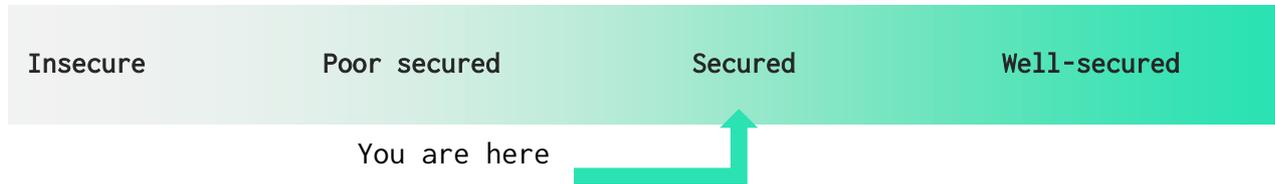


Functional review

- Business Logics Review
- Functionality Checks
- Access Control & Authorization
- Escrow manipulation
- Token Supply manipulation
- Asset's integrity
- User Balances manipulation
- Kill-Switch Mechanism
- Operation Trails & Event Generation

Executive Summary

According to the assessment, the Customer's smart contracts are secured but could have increased gas fees

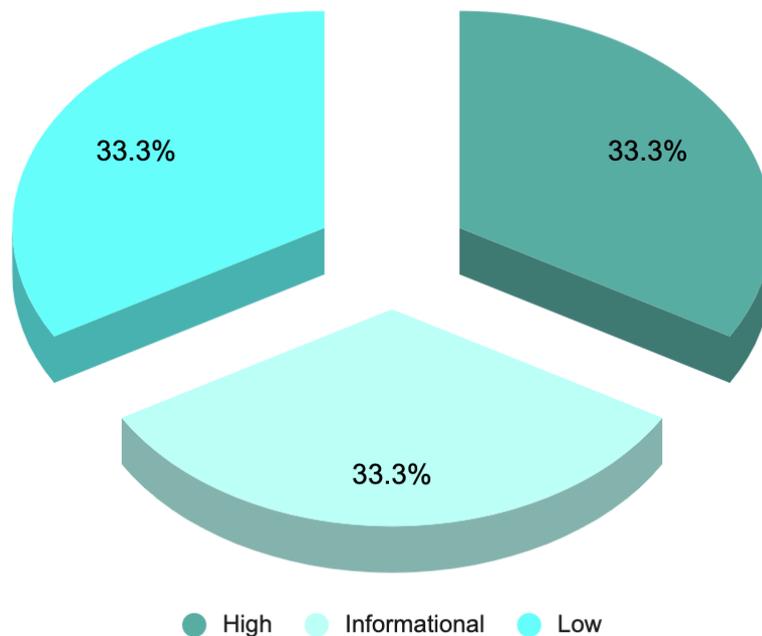


Our team performed an analysis of code functionality, manual audit, and automated checks with Mythril and Slither. All issues found during automated analysis were manually reviewed, and important vulnerabilities are presented in the Audit overview section. All found issues can be found in the Audit overview section.

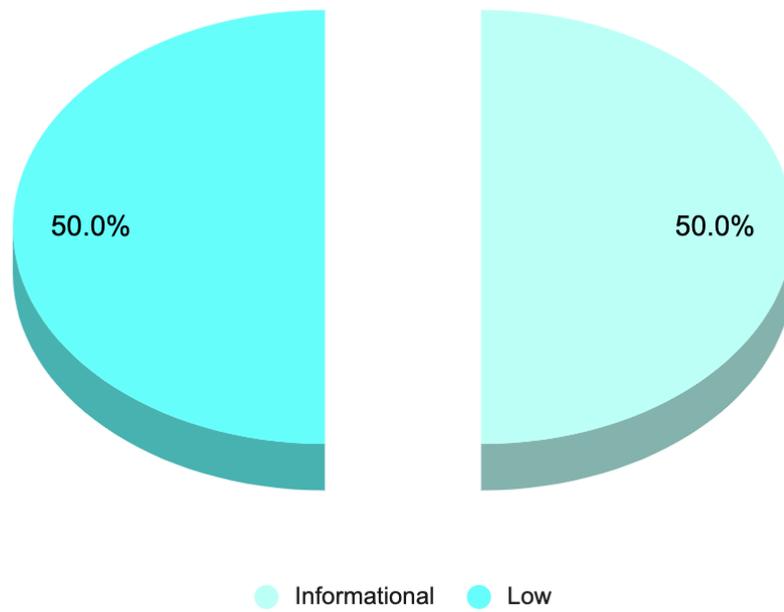
Security engineers found 1 high, 1 low and 1 informational issues during the first review.

Security engineers found 1 low and 1 informational issue during the second review.

Graph 1. The distribution of vulnerabilities after the first review.



Graph 2. The distribution of vulnerabilities after the second review.



Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
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 can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations, and info statements can't affect smart contract execution and can be ignored.

Audit overview

■ ■ ■ ■ Critical

No Critical severity issues were found.

■ ■ ■ High

1. Vulnerability: Reward allocation manipulation

while it's allowed to set `allocPoint` of the pool to zero (0), which will disallow all rewards and allowing to call `set` function with argument `_withUpdate` set to false, we see here possible reward allocation manipulation by the contract owner

Partially resolved by moving the ownership to the Timelock contract:
<https://bscscan.com/address/0xbd2a0bb757c7c6ea50f9e7eedb4b4350dec929e5#code>

■ ■ Medium

No Medium severity issues were found.

■ Low

1. Vulnerability: Costly loops

`massUpdatePools` may run out-of-gas if too many tokens are added. This may have implications on calling functions `add` and `set`.

Lines: MasterChef#1496-1501

```
function massUpdatePools() public {
    uint256 length = poolInfo.length;
    for (uint256 pid = 0; pid < length; ++pid) {
        updatePool(pid);
    }
}
```

■ Lowest / Code style / Best Practice

1. Vulnerability: Boolean equality

Boolean constants can be used directly and do not need to be compared to true or false.



Lines: MasterChef#1413-1416

```
modifier nonDuplicated(IBE20_lpToken) {  
    require(poolExistence[_lpToken] == false, "nonDuplicated:  
duplicated");  
    _;  
}
```



Conclusion

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security engineers found 1 high, 1 low and 1 informational issues during the first review.

Security engineers found 1 low and 1 informational issue during the second review.

Category	Check Items	Comments
→ Code Review	→ Style guide violation	→ boolean equality
	→ Costly loops	→ May run out-of-gas if many pools are added



Disclaimers

Hacken Disclaimer

The smart contracts given for audit have been analyzed 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).

The audit makes no statements or warranties on 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 platform. The platform, its programming language, and other software related to the smart contract can have its vulnerabilities that can lead to hacks. Thus, the audit can't guarantee the explicit security of the audited smart contracts.