HACKEN

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: FOTA
Date: November 15th, 2021

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Document

Name	Smart Contract Code Review and Security Analysis Report for FOTA.
Approved by	Andrew Matiukhin | CTO Hacken OU
Type	ERC20 token sale
Platform	Binance Smart Chain / Solidity
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Repository	https://github.com/fotaio/sale-contracts
Commit	5c252d5964298fda2a563e8724ccd888cd1af047
Deployed contract	https://bscscan.com/address/0xe4D810feb232eA08373a79A826b4955D72732f10#code https://bscscan.com/address/0x9d13B363D0349681F397570673E68006890CdDf8#code https://bscscan.com/address/0x6dC21054A413BE08E8d8bb6ce1B87358D0e3C9E3#code https://bscscan.com/address/0x0d9D43618e695Fbc3116E59CF456381fC0330A8F#code https://bscscan.com/address/0x1ddB673873FeCBCEe05A3F424a6528d956c4B6c9#code https://bscscan.com/address/0x40a80000d5CADa0A03F8fAC8931eEBD8D4Eedc54#code
Technical Documentation	NO
JS tests	NO
Timeline	02 NOVEMBER 2021 - 09 NOVEMBER 2021
Changelog	09 NOVEMBER 2021 - Initial Audit 15 NOVEMBER 2021 - Second Review

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Table of contents

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Introduction

Hacken OÜ (Consultant) was contracted by FOTA (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of the Customer's smart contract and its code review conducted between November 02nd, 2021 - November 09th, 2021.

Second review conducted on November 15th, 2021.

Scope

The scope of the project is smart contracts in the repository:

Repository:
https://github.com/fotaio/sale-contracts
Commit:
5c252d5964298fda2a563e8724ccd888cd1af047
Technical Documentation: No
JS tests: Yes, in the repository
Contracts:
SeedSale.sol
StrategicSale.sol
PrivateSale.sol
interfaces/IFOTAToken.sol
libs/fota/Auth.sol
libs/zeppelin/token/BEP20/IBEP20.sol

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

Category	Check Item
Code review	▪ 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 ▪ Assets integrity ▪ User Balances manipulation ▪ Data Consistency manipulation ▪ Kill-Switch Mechanism ▪ Operation Trails & Event Generation

Executive Summary

According to the assessment, the Customer's smart contracts are well-secured.

Insecure	Poor secured	Secured	Well-secured

You are here

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.

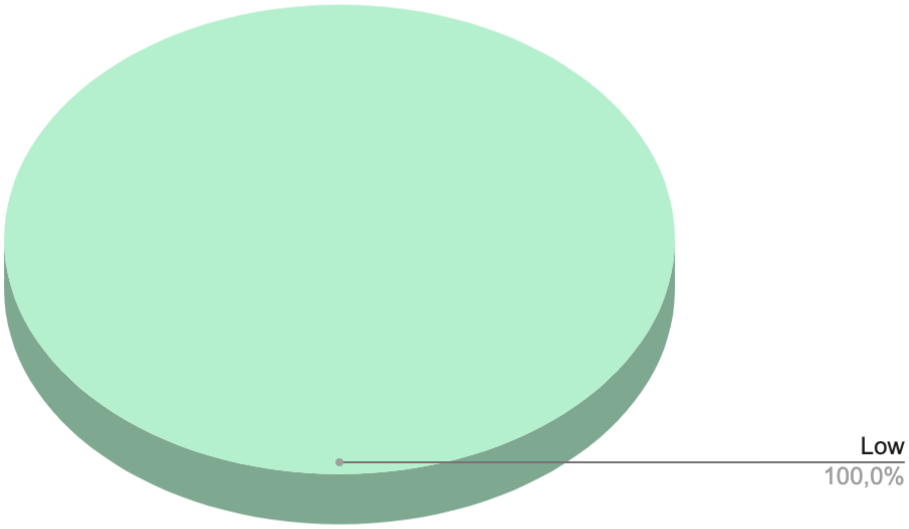
As a result of the audit, security engineers found **1** medium and **3** low severity issues.

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

As a result of the second review, security engineers found **3** low severity issues.

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Graph 1. The distribution of vulnerabilities after the audit.



Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

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

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Audit overview

Critical

No critical issues were found.

High

No high severity issues were found.

Medium

1. Test runs not applicable

   Below contracts are required by tests but not available.

   Contracts: FOTAToken.sol, MBUSDToken.sol, MUSDTToken.sol

   Status: fixed

Low

1. Possible variable inconsistency

   Variable totalAllocated is not changed when buyer allocation removed.

   Contracts: PrivateSale.sol, SeedSale.sol, StrategicSale.sol

   Functions: removeBuyerAllocation

   Recommendation: Add changing totalAllocated to removeBuyerAllocation function.

2. Missing event for changing vestingTime, tgeRatio, fundAdmin

   Contracts: PrivateSale.sol, SeedSale.sol, StrategicSale.sol

   Functions: updateVestingTime, updateTGERatio, updateFundAdmin

   Changing critical values should be followed by the event emitting for better tracking off-chain.

   Recommendation: Please emit events on the critical values changing.

3. A public function that could be declared external

   public functions that are never called by the contract should be declared external to save gas.

   Contracts: PrivateSale.sol, SeedSale.sol, StrategicSale.sol

   Function: initialize

   Recommendation: Use the **external** attribute for functions never called from the contract.

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Conclusion

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

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

As a result of the audit, security engineers found **1** medium and **3** low severity issues.

As a result of the second review, security engineers found **3** low severity issues.

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

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 the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug-free 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 the security of smart contracts.

Technical Disclaimer

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