HACKEN

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: Solarminex
Date: November 22nd, 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 Solarminex.
Approved by	Andrew Matiukhin | CTO Hacken OU
Type	ERC20 token with fees
Platform	Ethereum / Solidity
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Repository	https://github.com/cryptowelts/solarminex/blob/main/Solarminex.sol
Commit	4d04cb0ddc6c0cdc0437faa6ffc2f4c227fd702f
Technical Documentation	YES
JS tests	NO
Website	Solarminex.com
Timeline	15 NOVEMBER 2021 - 22 NOVEMBER 2021
Changelog	16 NOVEMBER 2021 - INITIAL AUDIT 22 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 Solarminex (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 15th, 2021 - November 16th, 2021.

Second review conducted on November 22nd, 2021.

Scope

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

Repository:
https://github.com/cryptowelts/solarminex/blob/main/Solarminex.sol
Commit:
4d04cb0ddc6c0cdc0437faa6ffc2f4c227fd702f
Technical Documentation: Yes (whitepaper-en.pdf)
JS tests: No
Contracts:
Solarminex.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

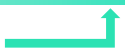
Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

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 **2** low severity issues.

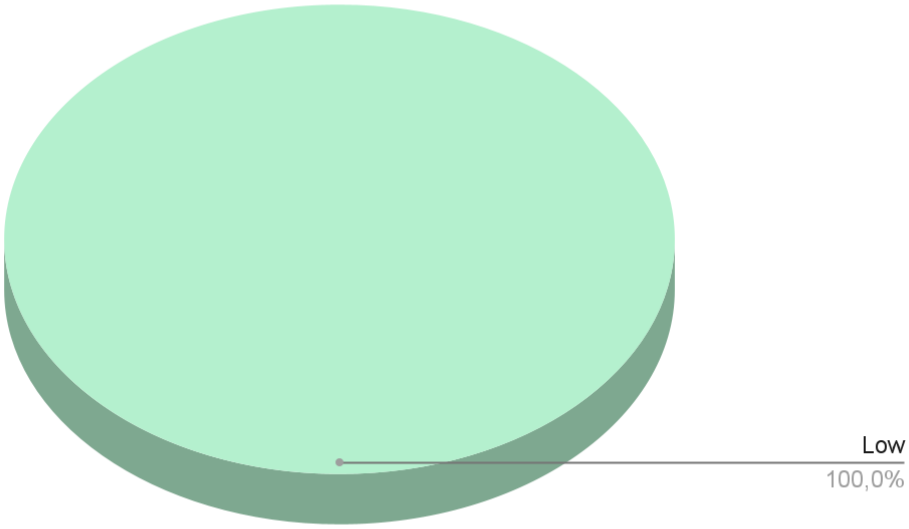
After the second review security engineers found that total supply was changed according to the whitepaper and the fee percentage was changed from 6 to 2. Therefore there are still **2** low severity issues.

Notice:

The Solarminex contract contains a transfer fee that is not described in the whitepaper.

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

Inconsistency with tokenomics.

In the provided whitepaper on page #18, there is a tokenomics. The tokenomics states: **TOTAL SUPPLY 1.500.000.000**. But in the code we can see the following on line #202:

```
uint256 private _totalSupply = 1E6 * 1E18;
```

While 1e6 means 1,000,000 and 1e18 just means the decimals (18 decimals for the token), so the total supply is less by 1,499,000,000 than it is declared in the whitepaper.

Contracts: Solarminex

Recommendation: Please make sure that the code is fully consistent with the whitepaper.

Status: Fixed

Low

1. The contract looks like an interface.

Abstract contract BPContract looks like an interface but is declared as “**abstract contract**”

Contracts: BPContract

Recommendation: Use keyword **interface** to declare interfaces in the code.

2. Fee not described in the whitepaper

The Solarminex contract contains a transfer fee that is not described in the whitepaper.

Recommendation: Please make sure that the code is fully consistent with the whitepaper.

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 **2** low severity issues.

After the second review security engineers found that total supply was changed according to the whitepaper and the fee percentage was changed from 6 to 2. Therefore there are still **2** low severity issues.

Notice:

The Solarminex contract contains a transfer fee that is not described in the whitepaper.

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.