SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: Nimbus
Date: May 30th, 2021

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

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 fixed – upon a decision of the Customer.

Document

Name	Smart Contract Code Review and Security Analysis Report for Nimbus.
Approved by	Andrew Matiukhin | CTO Hacken OU
Type	Swap
Platform	Ethereum / Solidity
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Repository	https://github.com/nimbusplatformorg/nim-smartcontract/tree/7bda71190cca5d139e15b46a33ca041eb060f38d (Initial Audit) https://github.com/nimbusplatformorg/nim-smartcontract/commit/6e57eafcdc7b9a08ccb0369bf135a69ce4680be5 (Remediation)
Commit	
Deployed contract	
Changelog	26 APR 2021 – Initial Audit 30 May 2021 – Remediation

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Hacken.

Table of contents

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Hacken.

Introduction

Hacken OÜ (Consultant) was contracted by Nimbus (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 April 26th, 2021. Remediation conducted on May 30th, 2021.

Scope

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

```
Repository: https://github.com/nimbusplatformorg/nim-smartcontract
Commit: 6e57eafcdc7b9a08ccb0369bf135a69ce4680be5

Files:
	Swaps/Factory.sol
	Swaps/LPRewards.sol
	Swaps/NBU_WETH.sol
	Swaps/Router.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

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Hacken.

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 secure.

Insecure	Poor secured	Secured	Well-secured

You are here ↑ (Secured)

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. A general overview is presented in AS-IS section, and all found issues can be found in the Audit overview section.

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

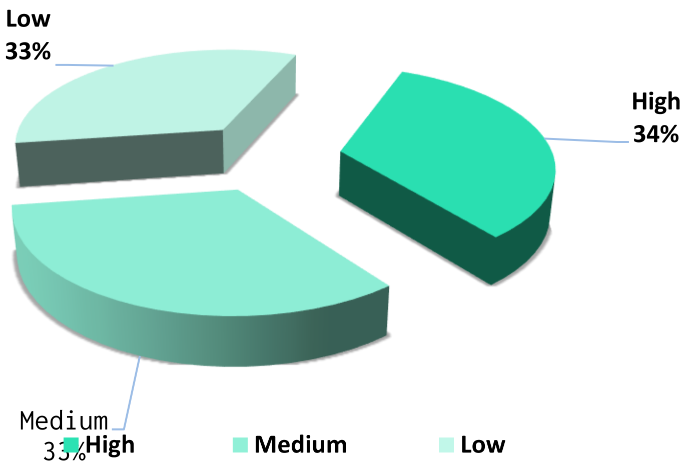
After the second review, the code contains 1 medium issue.

Notices:

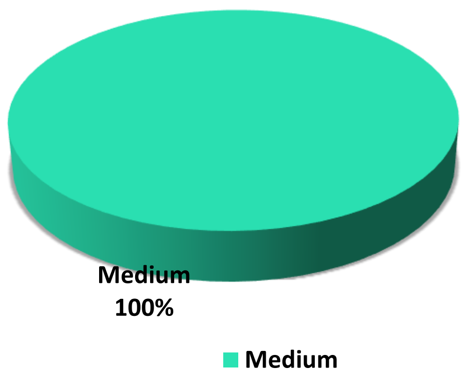
1. Description of custom logic is not provided, and we may not prove correctness of calculation.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Hacken.

Graph 1. The distribution of vulnerabilities after the audit.



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



This document is proprietary and confidential. No part of this document may be disclosed
in any manner to a third party without the prior written consent of Hacken.

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

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Hacken.

Audit overview

🟥 🟥 🟥 🟥 Critical

No critical issues were found.

🟨 🟨 🟨 High

1. The transfer function may fail if a msg.sender is the contract address with fallback function. As a result, funds may be locked.

   Contract: NBU_WETH

   Functions: withdraw

   Recommendation: stop using transfer() or send() and switch to using call() instead.

   Status: Addressed in 6E57EAFCDC7B9A08CCB0369BF135A69CE4680BE5 commit.

```
contract Vulnerable {
    function withdraw(uint256 amount) external {
        // This forwards 23000 gas, which may not be enough if the recipient
        // is a contract and gas costs change.
        msg.sender.transfer(amount);
    }
}

contract Fixed {
    function withdraw(uint256 amount) external {
        // This forwards all available gas. Be sure to check the return value!
        (bool success, ) = msg.sender.call.value(amount)("");
        require(success, "Transfer failed.");
    }
}
```

🟩 🟩 Medium

1. Usage of the custom WETH is not recommended. Such behavior can mislead users.

🟦 Low

1. The SafeMath library is redundant for compiler versions >= 8.0.0. All operations upon uint data type are checked.

   Contracts: all

   Recommendation: remove redundant libraries.

   Status: Addressed in 6E57EAFCDC7B9A08CCB0369BF135A69CE4680BE5 commit.

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.

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

After the second review, the code contains 1 medium issue.

Notices:

1. Description of custom logic is not provided, and we may not prove correctness of calculation.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Hacken.

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 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.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Hacken.