RAPID LABS

SMART CONTRACT SECURITY AUDIT

Final report **Plan: Simple**

Genesis Nomad Token

January 2024

RL@RAPIDLABS.FINANCE RAPIDLABS.FINANCE

TABLE OF CONTENTS

INTRODUCTION

The report has been prepared for Genesis Nomad Token.
Genesis Nomad Token is a reflect token. On each transfer a fee is taken. This fee is distributed amongst other holders proportional to their balances.
The token has a mechanism to auto-add liquidity. Is accumulates some fees on its balance, then sells half of them for the native currency and then adds the other part with native currency as liquidity.

Name	Genesis Nomad Token
Audit date	2024-01-17 - 2024-01-19
Language	Solidity
Platform	Binance Smart Chain

ANALYZED CONTRACTS

Name	Address
GenesisNomadToken	0x24D66Bd585510daCa4B1365da9d39E945ad413f9

AUDIT PROCESS

Our audit structure consists of two stages:

Auto-analysis

- Our automated tools allow us to scan smart contract code and find potential issues
- We hand pick and verify all the issues found by the tools

Expert audit

- Manual analysis of potential issues and vulnerabilities
- Contract code is reviewed thoroughly

KNOWN ISSUES CHECKED

Title	Result
Unencrypted Private Data On-Chain	✓ passed
Code With No Effects	✓ passed
Message call with hardcoded gas amount	✓ passed
Typographical Error	✓ passed
DoS With Block Gas Limit	✓ passed
Presence of unused variables	✓ passed
Incorrect Inheritance Order	✓ passed
Requirement Violation	✓ passed
Weak Sources of Randomness from Chain Attributes	✓ passed
Shadowing State Variables	✓ passed
Incorrect Constructor Name	✓ passed

Block values as a proxy for time	✓ passed
Authorization through tx.origin	✓ passed
DoS with Failed Call	✓ passed
Delegatecall to Untrusted Callee	✓ passed
Use of Deprecated Solidity Functions	✓ passed
Assert Violation	✓ passed
State Variable Default Visibility	✓ passed
Reentrancy	✓ passed
Unprotected SELFDESTRUCT Instruction	✓ passed
Unprotected Ether Withdrawal	✓ passed
Unchecked Call Return Value	✓ passed
Floating Pragma	✓ passed
Outdated Compiler Version	✓ passed
Integer Overflow and Underflow	✓ passed
Function Default Visibility	✓ passed

ISSUE CLASSIFICATION

High risk	Issues leading to assets theft, locking or any other loss of assets or leading to contract malfunctioning.
Medium risk	Issues that can trigger a contract failure of malfunctioning.
Low risk	Issues that do now affect contract functionality. For example, unoptimised gas usage, outdated or unused code, code style violations, etc.

ISSUES

High risk issues

No issues were found

Medium risk issues

No issues were found

Low risk issues

1. Iteration over array of unlimited length (GenesisNomadToken)

The function _getCurrentSupply() interates over an array with unlimited length

```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = rTotal;
    uint256 tSupply = tTotal;
    for (uint256 i = 0; i < excluded.length; i++) {
        if (rOwned[excluded[i]] > rSupply || tOwned[excluded[i]] > tSupply)
            return (rTotal, tTotal);
        rSupply = rSupply - rOwned[excluded[i]];
        tSupply = tSupply - tOwned[excluded[i]];
    }
```

```
            if (rSupply < rTotal / tTotal) return (rTotal, tTotal);
            return (rSupply, tSupply);
        }
```

This could lead to significant gas usage and in an extreme case the gas usage may be so big that the transaction would not fit in the block gas limit and token transfers may be blocked.

CONCLUSION

Genesis Nomad Token GenesisNomadToken contract was audited. 1 low risk issue was found.

DISCLAIMER

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without RapidLabs prior written consent.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts RapidLabs to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

RAPID LABS

YOUR PROJECT SECURED

RL@RAPIDLABS.FINANCE

RAPIDLABS.FINANCE