NOVOS

KYC & AUDIT.

Novos is an agency specializing in blockchain technology solutions, Audits, KYC / Doxx.

NOVOS

CERTIFICATE OF COMPLIANCE

Smart Contract Audit by NOVOS

BNBMINER | Audit Passed | July 21, 2022

NOVOS

Table of Contents

NOVOS

Audit Summary

This report has been prepared for BNBMINER on the Binance Chain network. Novos provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

NOVOS

Project Overview

Parameter	Result
Address	0x8CC881d68BD52c2F202133812Da5CC31D8439ab4
Name	BNBMINER
Platform	Binance Chain
Compiler	v0.4.26+commit.4563c3fc
Optimization	No with 200 runs
LicenseType	MIT license
Language	Solidity
Codebase	https://bscscan.com/address/0x8CC881d68BD52c2F202133812Da5CC31D8439ab4#code
Url	https://bnbminer.us/

Main Contract Assessed

Name	Contract	Live
BNBMINER	0x8CC881d68BD52c2F202133812Da5CC31D8439ab4	Yes

NOVOS

Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
❖ Unencrypted Private Data On-Chain	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Code With No Effects	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Message call with hardcoded gas amount	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Hash Collisions With Multiple Variable Length Arguments	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Unexpected Ether balance	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Presence of unused variables	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Right-To-Left-Override control character (U+202E)	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Typographical Error	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ DoS With Block Gas Limit	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Arbitrary Jump with Function Type Variable	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Insufficient Gas Griefing	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Incorrect Inheritance Order	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Write to Arbitrary Storage Location	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Requirement Violation	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Missing Protection against Signature Replay Attacks	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Weak Sources of Randomness from Chain Attributes	✓ Complete	✓ Complete	✓ **Low / No Risk**



NOVOS

Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
❖ Authorization through tx.origin	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Delegatecall to Untrusted Callee	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Use of Deprecated Solidity Functions	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Assert Violation	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Reentrancy	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Unprotected SELFDESTRUCT Instruction	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Unprotected Ether Withdrawal	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Unchecked Call Return Value	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Outdated Compiler Version	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Integer Overflow and Underflow	✓ Complete	✓ Complete	✓ **Low / No Risk**
❖ Function Default Visibility	✓ Complete	✓ Complete	✓ **Low / No Risk**



NOVOS

Contract Ownership

The contract ownership of BNBMINER is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.
.

01

The current owner is the address 0x59705ADD2C118af944589804084C5dF00aa3166d which can be viewed from: HERE

02

The owner wallet has the power to call the functions displayed on the priviliged functions chart below, if the owner wallet is compromised this privileges could be exploited.

03

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

NOVOS

Important Notes To The Users:

01 Market EGGS - 702298519630 uint256

02 Get My Eggs - 312190056129 uint256

03 BNB TO HATCH 1 MINERS - 540000 uint256

04 BNB_PER_MINERS_PER_SECOND=1; uint256 public BNB_TO_HATCH_1MINERS=540000;//for final version should be seconds in a day. uint256 PSN=10000; uint256 PSNH=5000;

05 Magic trade balancing algorithm function calculateTrade(uint256 rt,uint256 rs, uint256 bs) public view returns(uint256){ //(PSN*bs)/(PSNH+((PSN*rs+PSNH*rt)/rt))

06 Function seedMarket() public payable{ require(marketEggs==0); initialized=true; marketEggs=54000000000;

07 Function div(uint256 a, uint256 b) internal pure returns (uint256) { // assert(b > 0); // Solidity automatically throws when dividing by 0 uint256 c = a / b; // assert(a == b * c + a % b); // There is no case in which this doesn't hold return c

08 Substracts two numbers, throws on overflow (i.e. if subtrahend is greater than minuend). */ function sub(uint256 a, uint256 b) internal pure returns (uint256) { assert(b <= a); return a - b;

09 Adds two numbers, throws on overflow. */ function add(uint256 a, uint256 b) internal pure returns (uint256) { uint256 c = a + b; assert(c >= a); return c;.

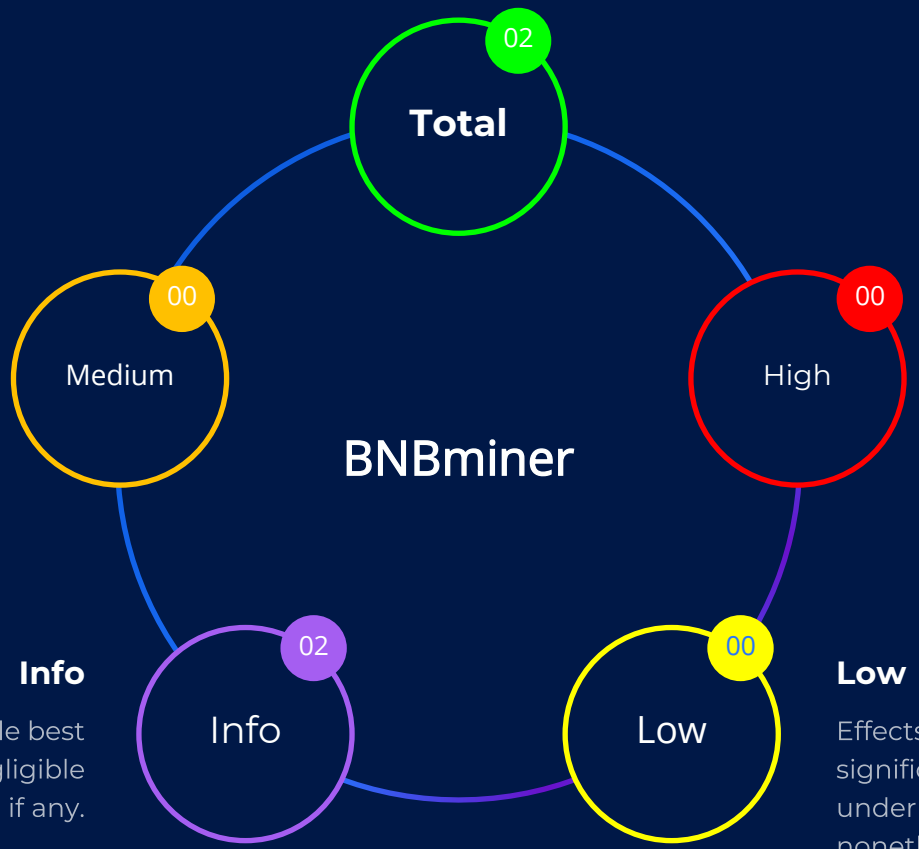
NOVOS

Technical Findings Summary

Classification of Issues

Total

What you should pay attention to



Medium

Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.

High

Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency

Info

Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

Low

Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.

NOVOS

Disclaimer

Novos has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and Novos is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will Novos or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by Novos is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where- is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.