4 Oct 2022

DRIVENsecurity
Premium Audit

Rev3al

Static Code Analysis & Manual
Verification For Smart Contract

WWW.DRIVENECOSYSTEM.COM

Disclaimer

Accepting a project audit can be viewed as a sign of confidence and is typically the first indicator of trust for a project, but it does not guarantee that a team will not remove all liquidity, sell tokens, or engage in any other type of fraud. There is also no method to restrict private sale holders from selling their tokens. It is ultimately your obligation to read through all documentation, social media posts, and contract code for each particular project in order to draw your own conclusions and define your own risk tolerance.

DRIVENlabs Inc. accepts no responsibility for any losses or encourages speculative investments. This audit's material is given solely for information reasons and should not be construed as investment advice.

Table Of Contents

Project Details

Name of the project:
Rev3al

Type of the Smart Contract:
Custom BEP20 token

Chain:
Binance Smart Chain

Address:
0x30B5E345C79255101B8af22a19805A6fb96DdEBb

Explorer Link:
https://bscscan.com/address/0x30b5e345c79255101b8af22a19805a6fb96ddebb

Static Analysis

SWC ISSUES	STATUS
Function Default Visibility	PASSED
Integer Overflow and Underflow	PASSED
Outdated Compiler Version	PASSED
Floating Pragma	PASSED
Unchecked Call Return Value	PASSED
Unprotected Ether Withdrawal	PASSED
Unprotected SELFDESTRUCT Instruction	PASSED
Reentrancy	PASSED
State Variable Default Visibility	PASSED
Uninitialized Storage Pointer	PASSED
Assert Violation	PASSED
Use of Deprecated Solidity Functions	PASSED
Delegatecall to Untrusted Callee	PASSED
DoS with Failed Call	PASSED
Transaction Order Dependence	PASSED
Authorization through tx.origin	PASSED
Block values as a proxy for time	PASSED
Signature Malleability	PASSED
Incorrect Constructor Name	PASSED
Shadowing State Variables	PASSED
Weak Sources of Randomness from Chain Attributes	PASSED
Missing Protection against Signature Replay Attacks	PASSED
Lack of Proper Signature Verification	PASSED
Requirement Violation	PASSED

Static Analysis

SWC ISSUES	STATUS
Write to Arbitrary Storage Location	PASSED
Incorrect Inheritance Order	PASSED
Insufficient Gas Griefing	PASSED
Arbitrary Jump with Function Type Variable	PASSED
DoS With Block Gas Limit	PASSED
Typographical Error	PASSED
Right-To-Left-Override control character (U+202E)	PASSED
Presence of unused variables	PASSED
Unexpected Ether balance	PASSED
Hash Collisions With Multiple Variable Length Arguments	PASSED
Message call with hardcoded gas amount	PASSED
Code With No Effects	PASSED

Issues

Static Code Analysis

No isseues found.

Manual Verification

No isseues found.

Functions

Only-owner functions

- blockAddress - lock a hacked address (can’t block a DEX/CEX address);
- unblockAddress - unlock an address;
- setDexAddress - mark an address as CEX/DEX;
- toggleStaking - start/stop staking;
- blockMultiple / unblockMultiple - lock/unlock multiple addresses;
- changeAPR - change the APR of inherited staking function;
- setStakingSupply - set the allocated amount for staking;
- withdrawWrongTokens - withdraw ERC20 tokens that were sent by mistake to the smart contract;

Functions for users

- stakeTokens - stake tokens for 30/180/365 days;
- unstakeTokens - unstake tokens from a given deposit;
- emergencyWithdraw - unstake tokens without receiving rewards;
- selfReport - allow users to self report their address if it was compromised;

Internal functions

- _transfer - Overrides the standard transfer function of the inherited ERC20 smart contract;

Observations

The smart contract inherits a staking mechanism, allowing users to stake their tokens without sending them to a third-party smart contract (MasterChef).

The smart contract poses no risk because the staking functions are protected by the "callersUser" and "nonReentrant" modifiers, which prevent any smart contract/wallet from interacting with the smart contract maliciously.

The _transfer function was modified so that if a user self-reports its address, the chances of recovering the stolen funds are increased. Furthermore, a user who staked tokens will retain the full amount in their wallet but will only be able to transfer the amount that was not staked.

Conclusion

On the technical side, the Rev3al smart contract poses no risk and can currently be traded freely on centralized and decentralized exchanges. The additional features added to the new smart contract were designed to mitigate the majority of the risks.

4 Oct 2022

Thank you!

Request a complete audit
www.drivenecosystem.com/drivensecurity