4 Oct 2022

DRIVENsecurity
Technical Audit

BridgeDeFi

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:
BridgeDeFi

Type of the Smart Contract:
Custom Smart Contract

Chain:
Goerli Testnet

Address:
0xba12A42E4E1FFA754c70C8814BE3Bb0d9C8f498d

Explorer Link:
https://goerli.etherscan.io/address/0xba12A42E4E1FFA754c70C8814BE3Bb0d9C8f498d#code

Static Analysis

SWC ISSUES	STATUS
Function Default Visibility	PASSED
Integer Overflow and Underflow	PASSED
Outdated Compiler Version	PASSED
Floating Pragma	LOW-SEVERITY
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
“A Floating Pragma is set” - does not represent a security risk.

Manual Verification
No isseues found.

Functions

Functions

- addProfits - add profits to a company and distribute them in the same transaction; It's called the "distributePorfits" internal function in order to send BUSD to NFT holders (parameter called from the Bridge smart contract - getNFTHoldersArray).

Conclusion

The distribution.sol smart contract is used to receive BUSD and distribute it to NFT holders. There is no risk of losing funds because this smart contract only works if the user sends BUSD at the time of calling the "addProfits" function.

4 Oct 2022

Thank you!

Request a complete audit
www.drivenecosystem.com/drivensecurity