Guard

Smart contracts security assessment

Preview Report

Retro INU

August 2022

0xguard.com

hello@0xguard.com

Contents

Introduction

The report has been prepared for Retro INU

Network	Binance Smart Chain
Contract type	ERC-20
Address	0x74779b656b7473f03c34ed51ef954aea2caa2b6f
Token name	Retro INU
Token symbol	RINU
Total supply	1000000000000
Decimals	9

Procedure

We perform our audit according to the following procedure:

Automated analysis

- Scanning the project's smart contracts with several publicly available automated Solidity analysis tools
- Manual verification (reject or confirm) all the issues found by the tools

Manual audit

- Manually analyze smart contracts for security vulnerabilities
- Smart contracts' logic check

Known vulnerabilities checked

Title	Check result
Unencrypted Private Data On-Chain	passed
Code With No Effects	
Message call with hardcoded gas amount	
Typographical Error	
DoS With Block Gas Limit	passed
Presence of unused variables	
Incorrect Inheritance Order	
Requirement Violation	
Weak Sources of Randomness from Chain Attributes	passed
Shadowing State Variables	
Incorrect Constructor Name	
Block values as a proxy for time	
Authorization through tx.origin	
DoS with Failed Call	
Delegatecall to Untrusted Callee	
Use of Deprecated Solidity Functions	
Assert Violation	
State Variable Default Visibility	
Reentrancy	
Unprotected SELFDESTRUCT Instruction	
Unprotected Ether Withdrawal	
Unchecked Call Return Value	

Conclusion

Retro INU was audited. 0 high, □ medium, □ low severity issues were found. Users should check if they interact with the same contracts as were audited.

This is a preview of an audit report. Please contact us to get a full report in less than 24 hours!

Classification of issue severity

High severity	High severity issues can cause a significant or full loss of funds, change of contract ownership, major interference with contract logic. Such issues require immediate attention.
Medium severity	Medium severity issues do not pose an immediate risk, but can be detrimental to the client's reputation if exploited. Medium severity issues may lead to a contract failure and can be fixed by modifying the contract state or redeployment. Such issues require attention.
Low severity	Low severity issues do not cause significant destruction to the contract's functionality. Such issues are recommended to be taken into consideration.

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 0xGuard 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 0xGuard 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.

0x Guard