Security Assessment

OpenBatchTransfer

Feb. 2nd, 2023

Table of Contents

1. Overview

1.1. Executive Summary

The OpenBatchTransfer contract is a permissionless contract to transfer ETH or ERC20 to multiple addresses in a single transaction.
We performed a comprehensive examination in combination of Static Analysis, Formal Verification and Manual Review techniques. In our review of the contract, no issues were identified.

1.2. Project Summary

Project Name	OpenBatchTransfer
Platform	Ethereum, Polygon
Language	Solidity
Code Repository	https://polygonscan.com/address/0x2cba9ad7e8a9268efe8049799597fdb22b6ed320

1.3. Assessment Summary

Delivery Date	Feb. 2nd, 2023
Audit Methodology	Static Analysis, Formal Verification, Manual Review
Auditor	Lee, Cara

1.4. Assessment Scope

ID	File
01	OpenBatchTransfer.sol

2. Checklist

2.1. General Vulnerability

Reentrancy	DelegateCall
Integer Overflow	Input Validation
Unchecked this.call	Frozen Money
Arbitrary External Call	Unchecked Owner Transfer
Do-while Continue	Right-To-Left-Override Character
Unauthenticated Storage Access	Risk For Weak Randomness
TxOrigin	Missing Checks for Return Values
Diamond Inheritance	ThisBalance
VarType Deduction	Array Length Manipulation
Uninitialized Variable	Shadow Variable
Divide Before Multiply	Function Not Working

2.2. Code Conventions

Compiler Version	Improper State Variable Modification
Function Visibility	Deprecated Function
Externally Controlled Variables	Code Style
Constant Specific	Event Specific
Return Value Unspecified	Nonexistent Error Message
Reference Variable Specification	Import Issue
Compare With Timestamp/Block Number/Blockhash	Constructor in Base Contract Not Implemented
Delete Struct Containing the Mapping Type	Usage of '=+'
Paths in the Modifier Not End with "_" or Revert	Non-payable Public Functions Use msg.value
SafeMath Issue	Compiler Error/Warning
ERC20/ERC721/ERC1155 Standard Specification	Anti-reentry Lock Specific
Nested Function Calls	Inheritance Issue
Signature Replay Risk	Missing Event

2.3. Gas Optimization

Tautology Issue	Loop Depends on Array Length
Redundant/Duplicated/Dead Code	Code Complexity/Code Inefficiency
Undeclared Resource	Optimizable Return Statement
Unused Resource	Duplicate Code

2.4. Compiler Bug

Affected by Compiler Bug

2.5. Logical Issue

The Code Implementation is Consistent With Comments, Project White Papers and Other Materials
Permission Check
Address Check

3. Findings

4. Disclaimer

No description, statement, recommendation or conclusion in this report shall be construed as endorsement, affirmation or confirmation of the project. The security assessment is limited to the scope of work as stipulated in the Statement of Work.

This report is prepared in response to source code, and based on the attacks and vulnerabilities in the source code that already existed or occurred before the date of this report, excluding any new attacks or vulnerabilities that exist or occur after the date of this report. The security assessment are solely based on the documents and materials provided by the customer, and the customer represents and warrants documents and materials are true, accurate and complete.

CONSULTANT DOES NOT MAKE AND HEREBY DISCLAIMS ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, REGARDING THE SERVICES, DELIVERABLES, OR ANY OTHER MATTER PERTAINING TO THIS REPORT.

CONSULTANT SHALL NOT BE RESPONSIBLE FOR AND HEREBY DISCLAIMS MERCHANTABILITY, FITNESS FOR PURPOSE, TITLE, NON-INFRINGEMENT OR NON-APPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY, SATISFACTORY QUALITY, ACCURACY, QUALITY, COMPLETENESS, TIMELINESS, RESPONSIVENESS, OR PRODUCTIVITY OF THE SERVICES OR DELIVERABLES.

CONSULTANT EXCLUDES ANY WARRANTY THAT THE SERVICES AND DELIVERABLES WILL BE UNINTERRUPTED, ERROR FREE, FREE OF SECURITY DEFECTS OR HARMFUL COMPONENTS, REVEAL ALL SECURITY VULNERABILITIES, OR THAT ANY DATA WILL NOT BE LOST OR CORRUPTED.

CONSULTANT SHALL NOT BE RESPONSIBLE FOR (A) ANY REPRESENTATIONS MADE BY ANY PERSON REGARDING THE SUFFICIENCY OR SUITABILITY OF SERVICES AND DELIVERABLES IN ANY ACTUAL APPLICATION, OR (B) WHETHER ANY SUCH USE WOULD VIOLATE OR INFRINGE THE APPLICABLE LAWS, OR (C) REVIEWING THE CUSTOMER MATERIALS FOR ACCURACY.

5. Appendix

5.1 Visibility

Contract	FuncName	Visibility	Mutability	Modifiers
OpenBatchTransfer	sendETH	external	Y	
OpenBatchTransfer	sendERC20Token	external	Y	
OpenBatchTransfer	rescueERC20	external	Y	
OpenBatchTransfer	rescueETH	external	Y	