IoTeX ioTube V6

Contract Audit Report

VER 1.1

7th June 2022

No. 2022060717371

Project Summary

1. Project Introduction

iotube V6 project based on Iotex chain can support multi-chain assets across chains. Users can obtain <crosscain erc20 v2> tokens by storing the tokens to be cross-chain in the <erc20tuberouter> or <crosscain erc20 v2pair> contract, and then store the <crosscain erc20 v2> tokens in the <erc20 tube> contract for destruction. Validators will sign the stored information hash after receiving the corresponding event. After collecting more than 2/3 of the validators' signatures, users can select the cross-domain erc20 V2 token in the target chain, and then obtain the target chain assets through <cross domain erc20 v2pair>.

2. Audit Summary

Project Name	IoTeX ioTube V6	**Platform**	N/A
Token	N/A	**Token symbol**	N/A
Start date	25 May 2022	**Language**	Solidity
End date	31 May 2022	**Website**	N/A
Github	github iotube-contracts 0f401c658a2202018e4198e27265e62ce9857b35	**Whitepaper**	N/A

3. Audit Scope

ID	File	SHA-256 checksum
contracts/v0.2	AssetRegistryV2.sol	5264eafe45db80e457a7ecf3a3415cb6b32668cc064088970187cc6e1462cba6
contracts/v0.2	CrosschainERC20FactoryV2.sol	e48adce3d145334b092093f1e97acb84808a36c1c17f180e294e265ef93159d8
contracts/v0.2	CrosschainERC20V2.sol	6e915861e065e1adff3e2a6674493e157f123aab680197ddbd17d4a8c03c5ca5
contracts/v0.2	CrosschainERC20V2Pair.sol	ffeaff1bc7c33960dec8bf11d4c61c016ce1a977daab0cb9a59450fd22fa288d
contracts/v0.2	ERC20Tube.sol	9c84b3bdb19c379e1be32dd5db48bbd3e9284a185b48d23ebf47547b3504ef75
contracts/v0.2	ERC20TubeRouter.sol	dd7fc9d3375864dd3e1aaabfdd4ac3c845a995747ca98fac7307849320344d05

ID	File	SHA-256 checksum
contracts/v0.2	EmergencyOperator.sol	433b34a5babcf5c0e134896768861fed3d84f51086784be246211c8c37150918
contracts/v0.2	LedgerV2.sol	aa1c9ebd2e7377e0cf27bbfbec06a50319ac7dbd03904c3fe1c962d59a11494b
contracts/v0.2	LordV2.sol	202d4eb5296a5bd21c80ae22750f9948c3254da7c4eb6e43451d922d929112c5
contracts/v0.2	MinterDAO.sol	5bbc2037e670d71f1a9a0c4ece2444da679fcf43a78991b7e8eb5c90e57f7339
contracts/v0.2	OwnedUpgradeable.sol	a934813ef9cc3e7531fe926ac07386e558386df7a0a6f6dcb5fa850a9880f618
contracts/v0.2	VerifierV2.sol	d732b76ad868060154d9255fe96f0131db873f8d6a514b3105f29f6597a1ea20

4. Code Structure

```
contracts/v0.2
├── AssetRegistryV2.sol
├── CrosschainERC20FactoryV2.sol
├── CrosschainERC20V2.sol
├── CrosschainERC20V2Pair.sol
├── ERC20Tube.sol
├── ERC20TubeRouter.sol
├── EmergencyOperator.sol
├── LedgerV2.sol
├── LordV2.sol
├── MinterDAO.sol
├── OwnedUpgradeable.sol
└── VerifierV2.sol
```

Audit Report Summary

1. Audit Methods

The audit was conducted to gain a clear understanding of how the project was implemented and how it works. The audit team conducted in-depth research, analysis, and testing of the project code and collected detailed data. In this report, the audit team will list in detail each issue identified, where it is located, the root cause of the issue, and a description of the issue, and will recommend changes to the issue accordingly.

Audit methods	Static analysis, Manual Review

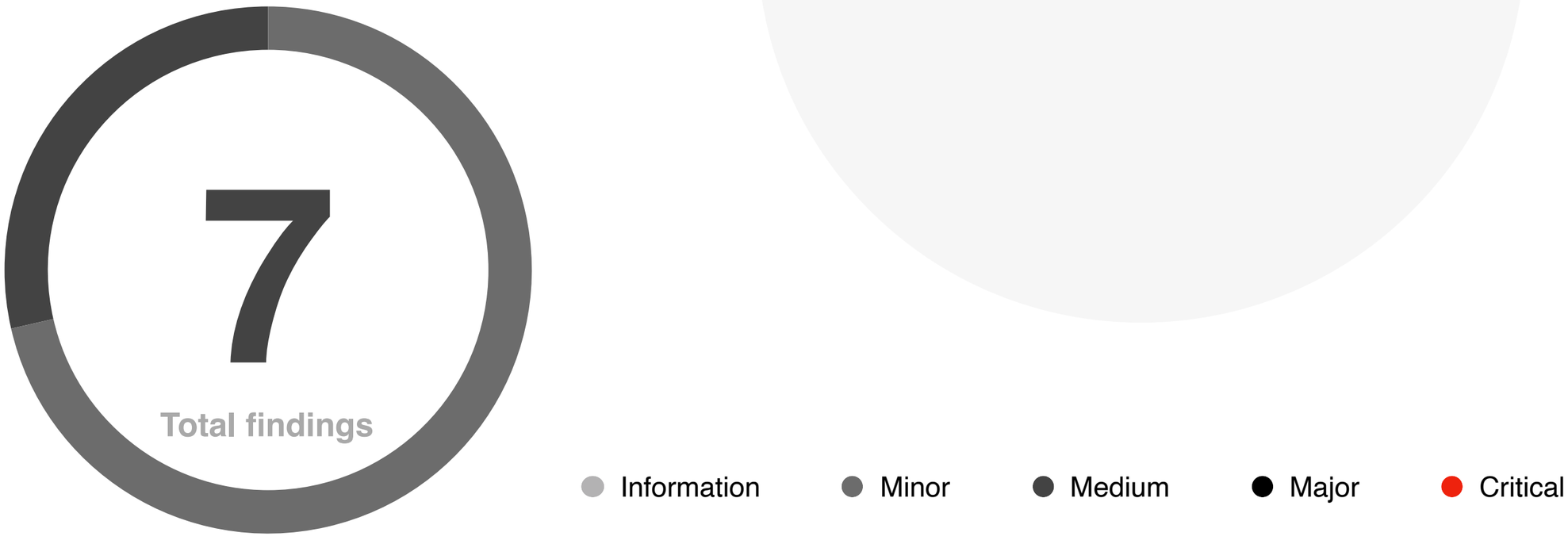
2. Audit Process

Steps	Operation	Description
1	Background	Read project descriptions, white papers, contract source code, and other relevant information the project team provides to ensure a proper understanding of project functions.
2	Automated testing	Scanning source code mainly with automated tools to find common potential vulnerabilities.
3	Manual reveiw	Engineers read the code line by line to find potential vulnerabilities.
4	Logical proofread	The engineer will compare the understanding of the code with the information provided by the project and check whether the code implementation is in line with the project white paper information.
5	Test case	Including test case design, test scope analysis, symbolic execution, etc.
6	Optimization items	Review of projects in terms of maintainability, safety, and operability based on application scenarios, deployment methods, and latest research results.

3. Risk Levels

Risk level	Issue description
Critical	Fatal risks and hazards that need to fixed immediately.
Major	Some high risks and hazards that will lead to related problems that must be solved
Medium	Some moderate risks and pitfalls may lead to potential risks that will eventually need to be addressed
Minor	There are low risks and hazards, mainly details of various types of mishandling or warning messages, which can be set aside for the time being
Information	Some parts can be optimized, such problems can be shelved, but it is recommended that the final solution

4. Audit Results



ID	Audit project	Risk level	Status
1	Reentrancy	None	
2	Injection	None	
3	Authentication bypass	None	
4	MEV Possibility	None	
5	Revert	None	
6	Race condition	None	
7	Insufficient Gas Griefing	None	
8	The major impact of flash loans	None	
9	Unreasonable economic model	None	
10	Predictable random numbers	None	
11	Voting rights management confusion	None	

7th June 2022

ID	Audit project	Risk level	Status
12	Privacy leak	None	
13	Improper use of time on chain	None	
14	Improper codes in fallback function	None	
15	Improper identification	None	
16	Inappropriate opcode	None	
17	Inappropriate assembly	None	
18	Constructor irregularities	None	
19	Return value irregularity	None	
20	Event irregularity	None	
21	Keywords irregularity	None	
22	Not following ERC standards	None	
23	Irregularity of condition judgment	None	
24	Risk of liquidity drain	None	
25	Centralization Risk	None	
26	Logic change risk	None	
27	Integer overflow	None	
28	Improper function visiblity	None	
29	Improper initialization of variables	None	
30	Improper contract calls	Minor	**Resolved**
31	Variable irregularities	None	
32	Replay	None	
33	Write to Arbitrary Storage Location	None	
34	Honeypot logic	None	
35	Hash collision	None	
36	Improper reward logic	None	
37	Deprecated methods used	None	
38	Coding principles break	None	
39	Code logic issue	Medium	**Partial Resolved**
40	Asset security	Minor	**Resolved**

*In the above table, if the status column is “**Acknowledged**”, the audit team has informed the project owner of the vulnerability. Still, the project owner has not made any changes to the vulnerability or has not announced to the audit team the progress of the changes to the vulnerability. If the status column is “**Resolved**”, the project owner has changed the exposure, and the audit team has confirmed the changes.

7th June 2022

5. Risk and Modification Program

The following section provides detailed information about the risk items learned after the audit, including the type of risk, risk level, location of the issue, description of the problem, recommendations for changes, and feedback from the project owner.

Risk type	Code logic issue	Risk level	Medium
Location	Line 146	**Contract file**	AssetRegistryV2.sol
Description	In the <deactivatetube> function, <activetubeids[\u id]> is assigned to true		
Recommedation	<activetubeids[\u id]> in the <deactivatetube> function should be assigned false		
Update	Fixed		

Risk type	Code logic issue	Risk level	Medium
Location	Line 22	**Contract file**	LedgerV2.sol
Description	In the <removeoperator> function, <operators[operator]> is assigned to true		
Recommedation	<operators[operator]> in the <removeoperator> function should be assigned false		
Update	Fixed		

Risk type	Asset security	Risk level	Minor
Location		**Contract file**	CrosschainERC20V2Pair.sol
Description	The <deposit> and <deposit to> operations in this contract will accumulate the small amount of assets brought about by the user due to non divisible. However, the current contract does not provide an interface for withdraw		
Recommedation	Add a contract interface to withdraw the accumulated assets; It can realize general token withdraw and solve the problem of deposit caused by mistakes		
Update	Fixed		

Risk type	Code logic issue	Risk level	Minor
Location	Line 65、91	**Contract file**	ERC20TubeRouter.sol
Description	The operation of <safe.transfer(msg.value)>uses the value <msg.value> when charging. If the user parameter is wrong, the tax will be overcharged		
Recommedation	Use <safe Transfer (setting.fee) > collect taxes, return excess assets, and check the return value		
Update	No Fix		

Risk type	Code logic issue	Risk level	Minor
Location	Line 98	**Contract file**	VerifierV2.sol
Description	<isValid_> is used to determine the number of validators whose valid signatures are greater than 2/3, but the minimum number of validators is not limited. When the value is 1, a single signature is judged to be valid		
Recommedation	Validators should be limited Minimum value of length		
Update	No Fix		

Risk type	Improper contract calls	Risk level	Minor
Location	Line 97、94	**Contract file**	ERC20Tube.sol ERC20TubeRouter.sol
Description	The return value of transferfrom call is not determined		
Recommedation	Judge the return value of <transferfrom>		
Update	Fixed		

Risk type	0 address check	Risk level	Minor
Location	Line 29、34 Line 20 Line 25 Line 44、52 Line 71、167	**Contract file**	CrosschainERC20FactoryV2.sol MinterDAO.sol OwnedUpgradeable.sol ERC20TubeRouter.sol ERC20Tube.sol
Description	Address is used as input parameter to set status variable, and address validity is not checked		
Recommedation	Check that the address is < non-0> address		
Update	Partial Fixed		

6. Recommendation

N/A

7th June 2022

Disclaimer

i. This audit report focuses only on the types of audits identified in the final report issued. Other unknown security vulnerabilities are not part of this audit, and we do not accept responsibility for them.

ii. We shall only issue an audit report based on an attack or vulnerability that existed or occurred before the issuance of the audit report. We cannot determine the likely impact on the security posture of our projects for new attacks or vulnerabilities that may exist or occur in the future, and we are not responsible for them.

iii. The security audit analysis and other elements of our published audit report shall be based solely on documents and materials (including, but not limited to, contract codes) provided to us by the Project Party before the release of the audit report. Such documents and materials shall not be untrue, inaccurate, uninformative, altered, deleted, or concealed, and if the documents and materials provided by the Project Party are false, inaccurate, uninformative, changed, deleted or hidden, or if the documents and materials provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted or concealed, or if the documents and materials provided by the Project Party are uninformative, uninformative, altered, deleted or hidden. If the records and information provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted, or concealed, or if changes to such documents and information are made after the issuance of the audit report, we shall not be liable for any loss or adverse effect arising from any inconsistency between the reflected and actual conditions.

iv. The Project Parties are aware that our audit report is based on documents and information provided by the Project Parties and relies on the technology currently available. However, due to the technical limitations of any organization, there is a possibility that our audit report may not fully detect all risks. Our audit team encourages the project development team and any interested parties to conduct subsequent testing and audits of the project.

v. The project owner warrants that the project for which we are engaged to provide audit or testing services is legal, compliant, and does not violate applicable laws. The audit report is for the project owner's reference only, and the contents, manner of obtaining, use of, and any services or resources involved in the audit report shall not be relied upon for investment, tax, legal, regulatory, or advisory purposes of any kind, and we shall not be liable therefor. The Project Party shall not refer to, quote, display, or send the Audit Report in whole or in part to any third party without our prior written consent. The Project Party shall bear any loss or liability arising from that place. We assume no responsibility for any reliance on or use of the audit report for any purpose.

vi. This audit report does not cover the compiler of the contract or any areas beyond the programming language of the Smart Contract. The risk and liability of the audited Smart Contract arising from references to off-chain information or resources is the sole responsibility of the project party.

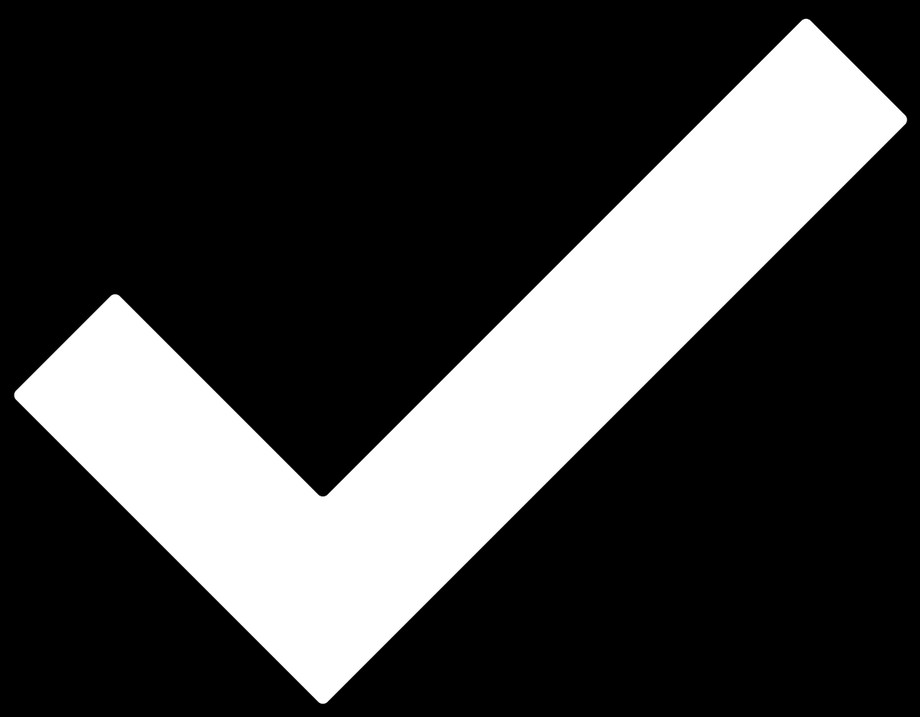
7th June 2022

vii. Force Majeure. Force majeure means an unforeseen event whose occurrence and consequences cannot be avoided and cannot be overcome by the parties at the time of entering into the contract, including but not limited to natural disasters such as war, typhoon, flood, fire, earthquake, tidal wave, lightning, natural disaster, strike, nuclear explosion, epidemic and other unforeseen events such as changes in laws, regulations and policies and governmental acts, whose occurrence and consequences cannot be prevented or avoided, and which contains, affects or delays the performance by either party of all or part of its obligations under the contract.

viii. Suppose either party believes that the occurrence of force majeure affects the performance of its obligations under this Agreement. In that case, it shall promptly notify the other party and, depending on the extent of the effect of the event on the performance of the Agreement; the parties shall consult to determine whether to terminate the Agreement or partially relieve itself of its obligations to perform the Agreement, or to extend the performance of the Agreement.

ix. In force majeure, neither party shall be deemed in breach or non-performance of its obligations under this Agreement. Any financial commitments existing before the event shall not be affected, and the project party shall make payment for work performed by us.

7th June 2022



Passed.

Date 7th June 2022

Audit Team 歐科雲鏈

The audit aims to review the asset cross-chain bridge function of iotube V6 version on the Iotex chain based on solidity, study its design and architecture, find potential security risks, and try to find possible vulnerabilities.