Security Assessment

iSwap V

Nov 29th, 2021

Table of Contents

Summary

This report has been prepared for iSwap to discover issues and vulnerabilities in the source code of the iSwap V project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	iSwap V
Platform	Ethereum, BSC, Heco, OKExChain, Polygon, Avax, FTM, Arbi
Language	Solidity
Codebase	https://github.com/dappiswap/iswap-bridge
Commit	159b0249e6245be474a7b5773d3c554e1438f674

Audit Summary

Delivery Date	Nov 29, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

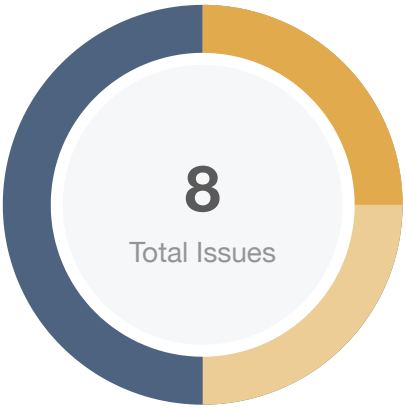
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
Major	0	0	0	0	0	0
Medium	2	0	0	2	0	0
Minor	2	0	0	0	0	2
Informational	4	0	0	3	0	1
Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
IHI	contracts/IHub.sol	54217004bc0486a44702687489456a1aae34a2914e4bd5c29afe2ea3c878f978
ISB	contracts/ISwapBaseBridge.sol	79b6c29cc79a45c33e6d0fc4cec451b574af8e3d16ce2ed252a2ea5e4e9bf6df

Findings



Critical	**0** (0.00%)
Major	**0** (0.00%)
Medium	**2** (25.00%)
Minor	**2** (25.00%)
Informational	**4** (50.00%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
IHI-01	Fees specified by the caller	Logical Issue	Minor	Resolved
IHI-02	Third Party Dependencies	Logical Issue	Informational	Acknowledged
IHI-03	Lack of Input Validation	Logical Issue	Informational	Acknowledged
IHI-04	Financial Models	Logical Issue	Minor	Resolved
IHI-05	Centralization Risk	**Centralization / Privilege**	**Medium**	Acknowledged
ISB-01	Third Party Dependencies	Logical Issue	Informational	Acknowledged
ISB-02	Financial Models	Logical Issue	Informational	Resolved
ISB-03	Centralization Risk	**Centralization / Privilege**	**Medium**	Acknowledged

IHI-01 | Fees specified by the caller

Category	Severity	Location	Status
Logical Issue	Minor	projects/ISwapV/contracts/IHub.sol (3056ada): 125, 179, 154	Resolved

Description

The fees in the transaction are specified by the function caller.

Recommendation

We suggest that the fees should be calculated or limited in the function.

Alleviation

The iSwap team heeded our advice and added the limitation for fees, and the change was supplied in commit `82095474a9275092465649abb55d83f8dcbd15c5`.

IHI-02 | Third Party Dependencies

Category	Severity	Location	Status
Logical Issue	Informational	projects/ISwapV/contracts/IHub.sol (3056ada): 215, 185, 151	Acknowledged

Description

The contract is serving as the underlying entity to interact with third party `WETH` protocols. The scope of the audit treats 3rd party entities as black boxes and assume their functional correctness. However, in the real world, 3rd parties can be compromised and this may lead to lost or stolen assets. In addition, upgrades of 3rd parties can possibly create severe impacts, such as increasing fees of 3rd parties, migrating to new LP pools, etc.

Recommendation

We understand that the business logic of `IHub` requires interaction with `WETH`. We encourage the team to constantly monitor the statuses of 3rd parties to mitigate the side effects when unexpected activities are observed.

Alleviation

[IHub]: We will keep notice the updates of `wrapperToken` to avoid vulnerabilities.

IHI-03 | Lack of Input Validation

Category	Severity	Location	Status
Logical Issue	Informational	projects/ISwapV/contracts/IHub.sol (3056ada): 140	Acknowledged

Description

The function `crossChainETH()` didn't check the `order.asset`. The relayer may call the function `refundToken()` and `crossChainConfirm()` according to the `order.asset`.

Recommendation

We suggest add the check on the `order.asset`.

Alleviation

[IHub]: Our backend program will judge the `order.asset` is whether reasonable according to which function the user called. If the user calls the function `crossChainETH()` and changes the `order.asset` to an unreasonable value, our backend program will still treat the `asset` as the `wrapperToken`.

IHI-04 | Financial Models

Category	Severity	Location	Status
Logical Issue	Minor	projects/ISwapV/contracts/IHub.sol (3056ada)	Resolved

Description

The main function of the `IHub` protocol can be listed as follows:

- Transfer the specified tokens to the user in the different chain.
- Transfer the platform token to the user in the different chain.
- Return the funds when the transaction failed.

And then, there are some questions:

1. The function `refundToken()` returns the amount `order.amount - gasFee` but the fees have already been transferred to the `treasury` address when the function `crossChainETH` and `crossChainToken` are called. It may cause a loss to the original funds in the contract.
2. The function `refundToken()` can work when the `srcOrderState` of order is 1. There are a lot of orders which have been successfully handled that can be used in the function `refund()`. It may cause a loss to the original funds in the contract.
3. The reliability of cross-chain swap depends on the relayers' reliability. It may have risks on this mechanism.

Recommendation

Financial models of blockchain protocols need to be resilient to attacks. They need to pass simulations and verifications to guarantee the security of the overall protocol.

The financial model of this protocol is not in the scope of this audit.

Alleviation

[IHub]: The user transfer his/her funds to the contract by the functions `crossChainETH()` and `crossChainToken()`. The contract will transfer the fees of transaction and gas to the `treasury` account. And meanwhile we will also transfer some tokens to the contract as the lower hold funds.

1. When we return funds to the user, the fees will from the lower hold funds.
2. Our backend program will judge whether the transaction can return funds to the user. The contract only judge the state of the order to avoid the problems with inconsistent data between the database

and blockchain which are caused by the rollback of block.

3. To sum up, the checks on the cross-chain transaction are in the hands of our backend program. Before the transaction, the program will calculate the fees of cross-chain and gas and return to the user. The user sign the data from the backend program and put it on the chain. If the user change the data from the backend program, the program will refund the user.

IHI-05 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	**Medium**	projects/ISwapV/contracts/IHub.sol (3056ada): 305, 294, 281, 274, 266, 260, 254, 249, 244, 238, 233, 229	Acknowledged

Description

In the contract `IHub`, the role `owner` has the authority over the following function:

- `pause()/unpause`: pause/unpause the function of cross-chain swap.
- `setRelayer()`: set the address of the `relayer`.
- `setTreasury()`: set the address to accept fees.
- `setCustodian()`: set the address of those who can withdraw the funds in the contract.
- `setRiskControl()`: set the address of role `RiskControl`.
- `setChainToken()`: set the address of `chainToken` which normally is the wrapped platform token.
- `setAssetCustodian()`: set the specified asset's custodian.
- `setAssetAmountMin()`: set minium amount of tokens every time transfer.
- `rescueETH()`: get the platform tokens.

And the role `custodian` has the authority to `withdraw` the tokens in the contract. And the role `RiskControl` has the authority to `withdrawPunish()` the tokens in the contract.

Any compromise to the `owner`, `custodian`, and `RiskControl` account may allow the hacker to take advantage of this.

Recommendation

We advise the client to carefully manage the `owner` account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

Indicatively, here is some feasible suggestions that would also mitigate the potential risk at the different level in term of short-term and long-term:

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;

- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

[iSwap Team]: We have a strict private key protection mechanism (signature machine mechanism), which is difficult to be attacked.

1. The private key is generated, encrypted, and stored by multiple parties. It can be accessed only after each party is authorized one by one;
2. During the signing process, we need to obtain partial private keys from multiple parties by encrypted transmission, and assemble them into the private key to complete the signature;
3. Hackers need to break the `ISwap` firewall first, then break multiple parties. Hackers need to break several symmetric and asymmetric encryption algorithms during this process, which is extremely difficult.

We have a strong emergency response mechanism:

1. We do not issue tokens and there are no user lock-ups, so user assets will not suffer losses;
2. We have a complete monitoring mechanism. When abnormal conditions such as the abnormal decrease of assets, loss of cross-chain transactions, inconsistent request hashes, etc. occur, the problem can be found within five minutes and resolved in time.

ISB-01 | Third Party Dependencies

Category	Severity	Location	Status
Logical Issue	Informational	projects/ISwapV/contracts/ISwapBaseBridge.sol (3056ada): 24, 239~240	Acknowledged

Description

The contract is serving as the underlying entity to interact with third party `DEX` and `ParamsParser` protocols. The scope of the audit treats 3rd party entities as black boxes and assume their functional correctness. However, in the real world, 3rd parties can be compromised and this may lead to lost or stolen assets. In addition, upgrades of 3rd parties can possibly create severe impacts, such as increasing fees of 3rd parties, migrating to new LP pools, etc.

Recommendation

We understand that the business logic of `IHub` requires interaction with `DEX` and `ParamsParser`. We encourage the team to constantly monitor the statuses of 3rd parties to mitigate the side effects when unexpected activities are observed.

Alleviation

iSwap team acknowledged this finding.

ISB-02 | Financial Models

Category	Severity	Location	Status
Logical Issue	Informational	projects/ISwapV/contracts/ISwapBaseBridge.sol (3056ada): 1	Resolved

Description

The main function of the `ISwap` protocol can be listed as follows:

- Normal token swap: the protocol provides the function of non-cross-chain token swap. The contract mainly uses the `AMM` contract to swap tokens.
- Cross-chain swap: the protocol provides the function of cross-chain token swap.
    1. Users transfer their tokens to the contract.
    2. The contract uses the `AMM` contract to swap the token from users to the `bridgeToken`.
    3. The relayer will call the function `confirmSwapCrossChain()` in the destination chain.
    4. The function `confirmSwapCrossChain()` will swap the `bridgeToken` to the token user want and the `AMM` will transfer those tokens to the user.

And then, there still are some questions:

1. What is the `relayer`? Are they programs or human? How did it work?
2. The transaction data is not stored in the block-chain. How to make sure the data will not change during the period processing the transaction?

Recommendation

Financial models of blockchain protocols need to be resilient to attacks. They need to pass simulations and verifications to guarantee the security of the overall protocol.

The financial model of this protocol is not in the scope of this audit.

Alleviation

[iSwap Team]: The `relayer` is our off-chain program. The key data of user transactions will be uploaded to the chain,including source chain exchange path, exchange quantity, minimum exchange quantity, selected dex, target chain selected dex, target chain receiver, minimum received quantity.

The key data in the business process will be uploaded to the chain to ensure that the user's data will not be tampered with. The exchange of the source chain is completely carried out on the chain.

The relayer will monitor the exchange result of the source chain. According to the exchange information of the target chain carried in the source chain transaction, the exchange transaction is initiated in the target chain contract. After the execution of the target chain contract is completed, the asset will be transferred to the target chain. Send to the target chain address specified in the source chain transaction to complete the cross-chain of assets.

ISB-03 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	**Medium**	projects/ISwapV/contracts/ISwapBaseBridge.sol (3056ada): 612, 594, 587, 580, 573, 564, 560, 529, 523, 507	Acknowledged

Description

In the contract `ISwapBaseBridge`, the role `owner` has the authority over the following function:

- `setBlackList()`: manage the blacklist.
- `setDexRouter()`: set the address of the `DEX Router`.
- `setDexRouterFunc()`: manage the function name of swapping tokens in different `DEX Router`.
- `pause()/unpause`: pause/unpause the function of cross-chain swap.
- `setRelayer()`: set the address of the `relayer`.
- `setTreasury()`: set the address to accept fees.
- `setCustodian()`: set the address of those who can withdraw the funds in the contract.
- `withdrawal()`: withdraw the tokens in the contract.
- `rescueETH()`: get the platform tokens.

And the role `custodian` has the authority to `withdraw` the tokens in the contract.

The role `RiskControl` has the authority to `withdrawPunish()` the tokens in the contract.

Any compromise to the `owner`, `custodian`, and `RiskControl` account may allow the hacker to take advantage of this.

Recommendation

We advise the client to carefully manage the `owner` account's private key to avoid any potential risks of being hacked.

In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

Indicatively, here is some feasible suggestions that would also mitigate the potential risk at the different level in term of short-term and long-term:

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;

- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

[iSwap Team]: We have a strict private key protection mechanism (signature machine mechanism), which is difficult to be attacked.

1. The private key is generated, encrypted, and stored by multiple parties. It can be accessed only after each party is authorized one by one;
2. During the signing process, we need to obtain partial private keys from multiple parties by encrypted transmission, and assemble them into the private key to complete the signature;
3. Hackers need to break the `ISwap` firewall first, then break multiple parties. Hackers need to break several symmetric and asymmetric encryption algorithms during this process, which is extremely difficult.

We have a strong emergency response mechanism:

1. We do not issue tokens and there are no user lock-ups, so user assets will not suffer losses;
2. We have a complete monitoring mechanism. When abnormal conditions such as the abnormal decrease of assets, loss of cross-chain transactions, inconsistent request hashes, etc. occur, the problem can be found within five minutes and resolved in time.

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

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 you ("Customer" or 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, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

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 CertiK 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.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS

AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING

MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.