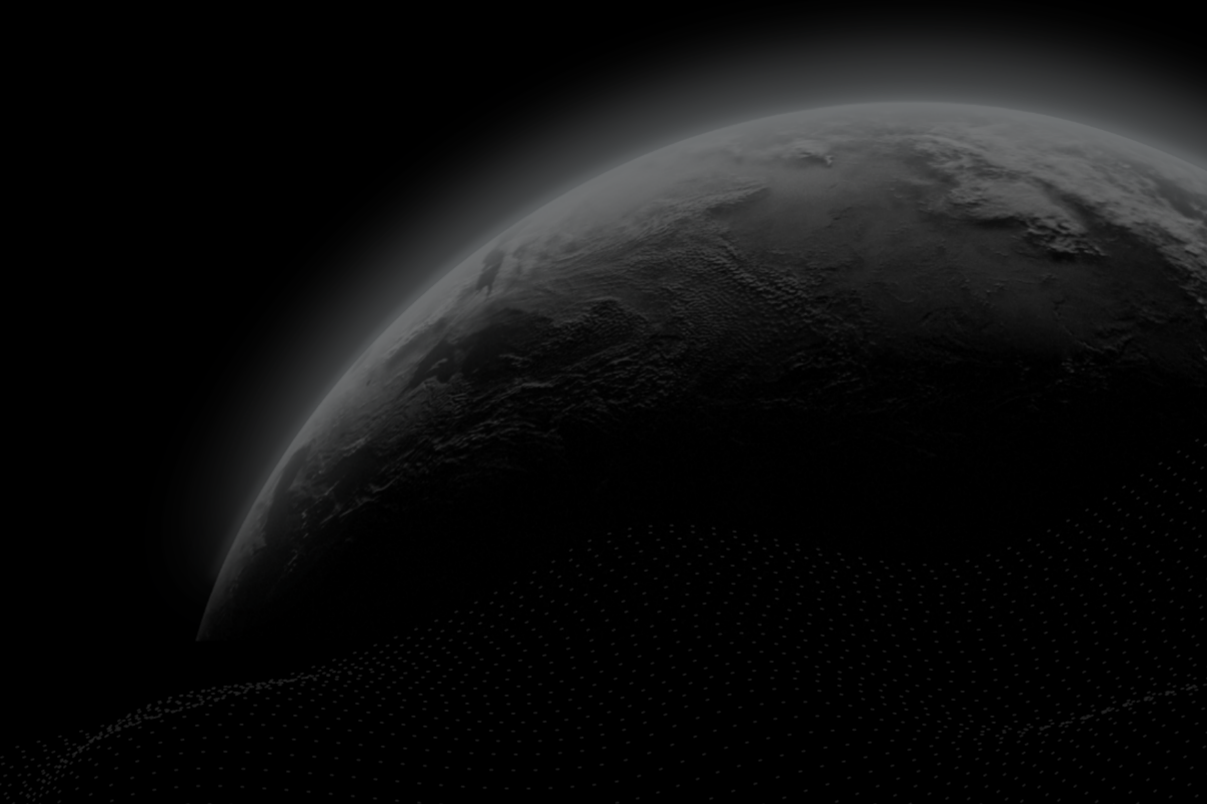
CERTIK

Security Assessment

Internet Money Swap Router - Ethereum

CertiK Verified on Mar 23rd, 2023



CertiK Verified on Mar 23rd, 2023

Internet Money Swap Router - Ethereum

The security assessment was prepared by CertiK, the leader in Web3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	Ethereum (ETH)	Formal Verification, Manual Review, Static Analysis

LANGUAGE	TIMELINE	KEY COMPONENTS
Solidity	Delivered on 03/23/2023	N/A

CODEBASE	COMMITS
https://bitbucket.org/internet-money/wallet-contracts/src/master/contracts/InternetMoneySwapRouter.sol ...View All	856179395047c7818b0b34ddae503089ba0c2969 8d6d9a771d0e7e6b6d3484174d2b788c64c0718e ...View All

Vulnerability Summary

3	0	1	1	1	0	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined	Unresolved

■	0	Critical		Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
■	1	Major	1 Mitigated	Major risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
■	1	Medium	1 Acknowledged	Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
■	1	Minor	1 Partially Resolved	Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions.
■	0	Informational		Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | INTERNET MONEY SWAP ROUTER - ETHEREUM

CODEBASE | INTERNET MONEY SWAP ROUTER - ETHEREUM

Repository

https://bitbucket.org/internet-money/wallet-contracts/src/master/contracts/InternetMoneySwapRouter.sol

Commit

856179395047c7818b0b34ddae503089ba0c2969

8d6d9a771d0e7e6b6d3484174d2b788c64c0718e

AUDIT SCOPE | INTERNET MONEY SWAP ROUTER - ETHEREUM

3 files audited ● 1 file with Acknowledged findings ● 1 file with Mitigated findings ● 1 file without findings

ID	File	SHA256 Checksum
● ORI	projects/Internet-money/wallet-contracts/contracts/OracleReader.sol	c671363505de84cabfc31b7217ca8daca3585a918570e51c72fcc188d40fedd0
● IMS	projects/Internet-money/wallet-contracts/contracts/InternetMoneySwapRouter.sol	5140ffbbdc6c5e01713b951552504c0ce1bfca097f8627f0ccc4df7dcaf652c4
● UIC	projects/Internet-money/wallet-contracts/contracts/Utils.sol	5e143ad7effd491847be81a4a4854ed6b554edfde11223ce2cdccd046952b72a

APPROACH & METHODS | INTERNET MONEY SWAP ROUTER - ETHEREUM

This report has been prepared for Internet Money to discover issues and vulnerabilities in the source code of the Internet Money Swap Router - Ethereum project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Formal Verification, Manual Review, and Static Analysis 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:

- Testing the smart contracts against both common and uncommon attack vectors;
- 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.

FINDINGS | INTERNET MONEY SWAP ROUTER - ETHEREUM

3	0	1	1	1	0
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Internet Money Swap Router - Ethereum. Through this audit, we have uncovered 3 issues ranging from different severity levels. Utilizing the techniques of Formal Verification, Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
IMS-01	**Centralization Related Risks**	**Centralization / Privilege**	**Major**	● **Mitigated**
ORI-01	Potential Flashloan Attack	Logical Issue	Medium	● Acknowledged
ICK-01	Third Party Dependency	Volatile Code	Minor	● Partially Resolved

IMS-01 | CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization / Privilege	● **Major**	**projects/Internet-money/wallet-contracts/contracts/Internet MoneySwapRouter.sol: 111, 136, 152, 165**	● **Mitigated**

Description

In the contract `InternetMoneySwapRouter` the role `_owner` has authority over the functions shown in the following functions:

- addDex()
- disableDex()
- updateTokenFee()

Any compromise to the `_owner` account may allow the hacker to take advantage of this authority and add/disable DEX supported, or change sensitive contract state data.

Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multisignature wallets. Indicatively, here are some feasible suggestions that would also mitigate the potential risk at a different level in terms of short-term, long-term and permanent:

Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND
- A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.
  AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles.
  OR
- Remove the risky functionality.

Alleviation

[Internet Money Team]:

We acknowledge that ownership is relevant in so far as enabling and disabling pathways to routers, however, relevant funds (native + wNative) are not accessible to the owner address.

We removed `updateTokenFee` and relaunch it if we find we need it again. Beyond this, we are not able to remove because it would go against our business logic, even though we do not plan to update outside of our first transactions.

Changes have been reflected in this commit.

ORI-01 | POTENTIAL FLASHLOAN ATTACK

Category	Severity	Location	Status
Logical Issue	● Medium	projects/Internet-money/wallet-contracts/contracts/OracleReader.sol: 90~102	● Acknowledged

Description

Flash loans are a way to borrow large amounts of money for a certain fee. The requirement is that the loans need to be returned within the same transaction in a block. If not, the transaction will be reverted.

An attacker can use the borrowed money as the initial funds for an exploit to enlarge the profit or manipulate the token price in decentralized exchanges.

The `checkPairForValidPrice` function relies on price calculations that are based on-chain, meaning they are susceptible to flash-loan attacks by manipulating the price of given (targetToken, _wNative) pairs to the attacker's benefit.

Scenario

- Let's say attacker A is a holder of `TimeDividend` tokens. He will get more dividend if the swap fees in `InternetMoneySwapRouter` increase.
- Victim user B initiates a swap request of token M to Token N, on the `InternetMoneySwapRouter` contract.
- A spots the swap transaction and front-runs that transaction with a flashloan-based price manipulation attack to the `(Token M -_wNative)` pool, pumping the price of Token M in that pool.
- Victim B has to pay much more fees due to the price manipulation, and attacker A will receive more dividends by holding `TimeDividend` tokens.
- Attacker A then pays back the flashloan. If the extra dividends he gained from the attack outweigh the costs, then he will have a financial incentive to perform such an attack.

Given that the auditor has no knowledge of how the back-end application estimates the swap fee, it is important to note that if the back-end relies on `getFeeMinimum()` to determine the fee attached to the transaction, then the aforementioned scenario is plausible.

Recommendation

If the project requires price references, caution should be taken to avoid flash loan attacks involving price manipulation. To minimize the chance of this happening, we recommend:

- using multiple reliable on-chain price oracle sources, such as Chainlink or Band protocol.

- using the Time-Weighted Average Price (TWAP). The TWAP represents the average price of a token over a specified time frame. If an attacker manipulates the price in one block, it will not affect the average price as drastically.

Alleviation

Internet Money team:

We are not concerned with fee loss or gain as much as we are with sandwich attacks that steal users funds. Users and clients are advised to utilize the minAmountOut to reduce their slippage.

ICK-01 | THIRD PARTY DEPENDENCY

Category	Severity	Location	Status
Volatile Code	● Minor	projects/Internet-money/wallet-contracts/contracts/InternetMoneySwapRouter.sol: 33; projects/Internet-money/wallet-contracts/contracts/OracleReader.sol: 17, 54, 90	● Partially Resolved

Description

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

```
33      Dex[] public dexInfo;
```

- The contract `InternetMoneySwapRouter` interacts with third-party contract with `IUniswapV2Router02` interface via `dexInfo`.

```
54      function amountOutFrom(address factory, address tokenIn, address tokenOut,
uint256 amountIn) public view returns(uint256) {
```

- The function `OracleReader.amountOutFrom` interacts with third-party contract with `IUniswapV2Factory` interface via `factory`.

```
 90      function checkPairForValidPrice(address factory, address token) public view
returns(uint256 tokenReserve, uint256 wethReserve) {
```

- The function `OracleReader.checkPairForValidPrice` interacts with third-party contract with `IUniswapV2Pair` interface via `factory`.

Recommendation

We understand that the business logic requires interaction with the third-party Dex protocols. We encourage the team to constantly monitor the statuses of third-party dependencies to mitigate the side effects when unexpected activities are observed.

Alleviation

The team implemented a check for `disabled` flag that make sure only the whitelisted dex address will be used in this contract.

Changes have been reflected in this commit.

OPTIMIZATIONS | INTERNET MONEY SWAP ROUTER - ETHEREUM

ID	Title	Category	Severity	Status
IMS-02	Redundant Code	Gas Optimization	Optimization	● Resolved

IMS-02 | REDUNDANT CODE

Category	Severity	Location	Status
Gas Optimization	● Optimization	projects/Internet-money/wallet-contracts/contracts/InternetMoneySwapRouter.sol: 56, 60	● Resolved

Description

`_wNative` is written twice, but not used in-between.

```
56          _wNative = wNative;
```

```
60          _wNative = wNative;
```

Recommendation

We recommend removing the writes of unused values.

Alleviation

The team heeded our advice and fixed the issue in this commit.

APPENDIX | INTERNET MONEY SWAP ROUTER - ETHEREUM

Finding Categories

Categories	Description
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.
Gas Optimization	Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.
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.
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

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 | CERTIK

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.

CertiK | Securing the Web3 World

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.