METATRUST

Security Assessment for

uniwhale

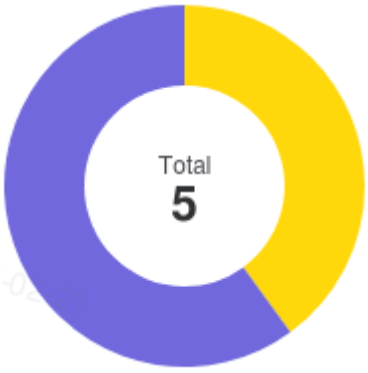
February 21, 2023

Executive Summary

Overview	
Project Name	uniwhale
Codebase Path	git://github.com/uniwhale
Scan Engine	Security Analyzer
Scan Time	2023/02/21 12:49:35
Source Code	uniwhale commit:-

Total	
Critical Issues	0
High risk Issues	0
Medium risk Issues	2
Low risk Issues	3
Informational Issues	0

Critical Issues	The issue can cause large economic losses, large-scale data disorder, loss of control of authority management, failure of key functions, or indirectly affect the correct operation of other smart contracts interacting with it.
High Risk Issues	The issue puts a large number of users' sensitive information at risk or is reasonably likely to lead to catastrophic impacts on clients' reputations or serious financial implications for clients and users.
Medium Risk Issues	The issue puts a subset of users' sensitive information at risk, would be detrimental to the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.
Low Risk Issues	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low-impact in view of the client's business circumstances.
Informational Issue	The issue does not pose an immediate risk but is relevant to security best practices or Defence in Depth.



Critical Issues	0%	0
High risk Issues	0%	0
Medium risk Issues	40%	2
Low risk Issues	60%	3
Informational Issues	0%	0

Summary of Findings

MetaScan security assessment was performed on **February 21, 2023 12:49:35** on project **uniwhale** with the repository **uniwhale** on branch **default branch**. The assessment was carried out by scanning the project's codebase using the scan engine **Security Analyzer**. There are in total **5** vulnerabilities / security risks discovered during the scanning session, among which **0** critical vulnerabilities, **0** high risk vulnerabilities, **2** medium risk vulnerabilities, **3** low risk vulnerabilities, **0** informational issues.

ID	Description	Severity	Alleviation
MSA-001	Centralized Roles	Medium risk	Acknowledged
MSA-002	Lack of check of salt in updateOpenOrder in RegistryCore.sol	Medium risk	Fixed
MSA-003	Incompatible with fee-charging token	Low risk	Fixed
MSA-004	Potential Redundant ETH Locked in the TradingCore Contract	Low risk	Acknowledged
MSA-005	Unused return value in contracts/LiquidityPool.sol	Low risk	Acknowledged

Findings

Critical (0)

No Critical vulnerabilities found here

High risk (0)

No High risk vulnerabilities found here

Medium risk (2)

1. Centralized Roles

Medium risk Security Analyzer

In the LiquidityPool contract, the centralized role owner has permission for the following functions:

- setSwapRouter: update the swapRouter;
- setMintFee:update the mintFee;
- setBurnFee: update the burnFee;
- collectAccruedFee: send the fee to the owner;
- pause:pause the contract;

In the LiquidityPool contract, the approved role has permission for the following functions:

- transferBase:transfer the baseToken token to arbitrage account;
- transferBaseFrom:transferbaseToken from an arbitrage account to another arbitrage account with the amount the from account approved to the LiquidityPool contract.

In the AbstractRegistry contract, the centralized role owner has permission for the following functions:

- setMaxOpenTradesPerPriceId: update the maxOpenTradesPerPriceId;
- setMaxOpenTradesPerUser: update the maxOpenTradesPerUser;
- setMaxMarginPerUser: update the maxMarginPerUser;
- setMinPositionPerTrade: update the minPositionPerTrade;
- setApprovedPriceId: update the approvedPriceId for the specified priceId;
- setLiquidationThresholdPerPriceId:update the liquidationThresholdPerPriceId for the specified priceId;
- setLiquidationPenalty: update the liquidationPenalty;
- setMaxLeveragePerPriceId:update the maxLeveragePerPriceId for the specified priceId;
- setMinLeveragePerPriceId: update the minLeveragePerPriceId for the specified priceId;
- setMaxPercentagePnLFloor:update the maxPercentagePnLFloor;
- setMaxPercentagePnLCap:update the maxPercentagePnLCap;
- setMaxPercentagePnLFactor: update the maxPercentagePnLFactor;
- setFee: update the fee;
- setFeeFactor: update the feeFactor;
- setStopFee: update the stopFee;
- setFundingFeePerPriceId: update the _fundingFeePerPriceId for the specified priceId;
- setImpactRefDepthLongPerPriceId: update the impactRefDepthLongPerPriceId for the specified priceId;
- setImpactRefDepthShortPerPriceId: update the impactRefDepthShortPerPriceId for the specified priceId;

In the RegistryCore contract, the centralized approved role has permission for the following functions:

- openMarketOrder:open a market order for the specified priceId;
- closeMarketOrder:close a market order for the specified order;
- updateOpenOrder: update a market order for the specified order;

In the TradingCore contract, the centralized role owner has permission for the following functions:

- pause:pause the contract;

- setOracleAggregator: set the oracleAggregator;

In the TradingCore contract, the centralized approved role has permission for the following functions:

- createTrade: create a trade;
- openMarketOrder(OpenTradeInput calldata openData,uint256 openPrice):open a market order;
- openMarketOrder(OpenTradeInput calldata openData, bytes[] calldata priceData): open a market order;
- closeMarketOrder:close a market order;
- addMargin: add some margin for an order;
- removeMargin: remove some for an order;

In the TradingCore contract, the centralized role liquidator has permission for the following functions:

- liquidateMarketOrder: liquidate a market order;

File(s) Affected

contracts/LiquidityPool.sol #15-19
contracts/interfaces/AbstractRegistry.sol #12-20
contracts/RegistryCore.sol #7-9
contracts/TradingCore.sol #18-23

Examples

```
15
16 contract LiquidityPool is
17   AbstractPool,
18   ERC20PausableUpgradeable,
19   ReentrancyGuardUpgradeable,
```

Recommendation

We advise using the multi-signature wallet and the timelock to mitigate the centralized role issue.

Alleviation Acknowledged

Owner will be a multisig/DAO contract, partially mitigating the centralisation risk

2. Lack of check of salt in updateOpenOrder in RegistryCore.sol

Medium risk Security Analyzer

When the updateOpenOrder is executed, the check of salt in order is missing, resulting in the fact that the orderHash and trade in the input parameter may not be the same order Normally, the salt in trade should be self-increasing. If the salt in trade is filled incorrectly, even if the orderhash is filled correctly, it will cause an unexpected order to be updated, which will cause a situation, that is, different orderhashes correspond to orders with the same information, or the same trade information corresponds to different orderhashes, which violates the requirements of data consistency

File(s) Affected

contracts/RegistryCore.sol #131-139

Examples

```
137   ) external override onlyRole(APPROVED_ROLE) {
138     Trade memory t = _openTradeByOrderHash[orderHash];
139
140     _require(t.user == trade.user, Errors.TRADER_OWNER_MISMATCH);
141     _require(t.priceId == trade.priceId, Errors.PRICE_ID_MISMATCH);
142     _require(t.isBuy == trade.isBuy, Errors.TRADE_DIRECTION_MISMATCH);
143
144     _openTradeByOrderHash[orderHash] = trade;
145     totalMarginPerUser[trade.user] = totalMarginPerUser[trade.user]
```

Recommendation

Add check of t.salt == trade.salt.

Alleviation Fixed

-

Low risk (3)

1. Incompatible with fee-charging token

Low risk Security Analyzer

If the tokenIn token is a deflationary token, the LiquidityPool contract received tokens will be less than the assigned number, amountIn , as a result, there is not enough tokenIn token can be swapped by the swapRouter . If the tokenIn token is a deflationary token, whether the function swapGivenIn supports the fee-charing tokens also counts.

File(s) Affected

contracts/LiquidityPool.sol #324-332

Examples

```
324          swapRouter.swapGivenIn(
325            ISwapRouter.SwapGivenInInput(
326              address(baseToken),
  •••
330              poolFee
331            )
332          )
```

Recommendation

If the client supports fee-charging tokens in the protocol now or in the future, we advise checking how many tokens the liquidity pool actually received and calling the 3rd party functions that support the fee-charging tokens.

Alleviation Fixed

-

2. Potential Redundant ETH Locked in the TradingCore Contract

Low risk Security Analyzer

A user needs to pay the updateFee to the oracleAggregator contract to get the price of opening or closing an order. However, there is no logic to return redundant ETH back to the user if the user paid more ETH to open or close an order

File(s) Affected

contracts/TradingCore.sol #20-25

Examples

```
20  contract TradingCore is
21    ITradingBook,
22    OwnableUpgradeable,
23    AccessControlUpgradeable,
24    ReentrancyGuardUpgradeable
25  {
```

Recommendation

We advise returning redundant ETH back to the user if there is.

Alleviation Acknowledged

this affects all contracts including payable and we will add appropriate withdrawl function as part of our book of work.

3. Unused return value in contracts/LiquidityPool.sol

Low risk Security Analyzer

Either the return value of an external call is not stored in a local or state variable, or the return value is declared but never used in the function body.

File(s) Affected

contracts/LiquidityPool.sol #247-285 #287-335

Examples

```
260       baseToken.transferFromFixed(sender, address(this), amountGross);
261     } else {
262       ERC20(tokenIn).transferFromFixed(sender, address(this), amountIn);
263       ERC20(tokenIn).approveFixed(address(swapRouter), amountIn);
264
265       amountGross = swapRouter.swapGivenIn(
266         ISwapRouter.SwapGivenInInput(
```

Recommendation

Ensure the return value of external function calls is used. Remove or comment out the unused return function parameters.

Alleviation Acknowledged

-

Informational (0)

No Informational vulnerabilities found here

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 MetaTrust'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 MetaTrust 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. MetaTrust's position is that each company and individual are responsible for their own due diligence and continuous security. MetaTrust'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 MetaTrust 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 Security Assessment AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, MetaTrust HEREBY DISCLAIMS ALL WARRANTIES,

WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, MetaTrust 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, MetaTrust 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, MetaTrust 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 MetaTrust NOR ANY OF MetaTrust'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. MetaTrust 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 MetaTrust'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 Security Assessment MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST MetaTrust WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF MetaTrust 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 MetaTrust 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.