



METATRUST

Draft  
Security Assessment for  
**115-2022-04-mimo  
(StaticFail) (1Positive-  
FLP)**

July 23, 2023

## Executive Summary

Overview			
Project Name	115-2022-04-mimo (StaticFail) (1Positive-FLP)		
Codebase URL	https://github.com/code-423n4/2022-04-mimo		
Scan Engine	AI Analyzer		
Scan Time	2023/07/23 17:06:50		
Commit Id	b18670f		






  

Total			
Critical Issues	0		
High risk Issues	5		
Medium risk Issues	0		
Low risk Issues	0		
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	100%	5
	Medium risk Issues	0%	0
	Low risk Issues	0%	0
	Informational Issues	0%	0

## Summary of Findings

MetaScan security assessment was performed on **July 23, 2023 17:06:50** on project **115-2022-04-mimo (StaticFail) (1Positive-FLP)** with the repository **<https://github.com/code-423n4/2022-04-mimo>** on branch **default branch**. The assessment was carried out by scanning the project's codebase using the scan engine **AI Analyzer**. There are in total **5** vulnerabilities / security risks discovered during the scanning session, among which **0** critical vulnerabilities, **5** high risk vulnerabilities, **0** medium risk vulnerabilities, **0** low risk vulnerabilities, **0** informational issues.

ID	Description	Severity
MSA-001	MWE-200: Insecure LP Token Value Calculation	High risk
MSA-002	MWE-200: Insecure LP Token Value Calculation	High risk
MSA-003	MWE-200: Insecure LP Token Value Calculation	High risk
MSA-004	MWE-200: Insecure LP Token Value Calculation	High risk
MSA-005	MWE-200: Insecure LP Token Value Calculation	High risk



## Findings

### Critical (0)

No Critical vulnerabilities found here

### High risk (5)

#### 1. MWE-200: Insecure LP Token Value Calculation

 High risk Security Analyzer

Liquidity token value/price can be manipulated to cause flashloan attacks.

##### File(s) Affected



core/contracts/oracles/GUniLPOracle.sol #91-125

```
91     function latestRoundData()
92     public
93     view
94     override
95     returns (
96         uint80 roundId,
97         int256 answer,
98         uint256 startedAt,
99         uint256 updatedAt,
100        uint80 answeredInRound
101    )
102    {
103        (, int256 answerA, , uint256 assetUpdatedAtA, ) = oracleA.latestRoundData();
104        (, int256 answerB, , uint256 assetUpdatedAtB, ) = oracleB.latestRoundData();
105        uint256 priceA = uint256(answerA);
106        uint256 priceB = uint256(answerB);
107        uint160 sqrtPriceX96 = uint160(
108            MathPow.sqrt((priceA.mul(_tokenDecimalsUnitB).mul(1 << 96)) / (priceB.mul(_tokenDecimalsUnitA)))
109        );
110
111        (uint256 rA, uint256 rB) = pool.getUnderlyingBalancesAtPrice(sqrtPriceX96);
112        require(rA > 0 || rB > 0, "C100");
113        uint256 totalSupply = pool.totalSupply();
114        require(totalSupply >= 1e9, "C101");
115
116        answer = int256(
117            priceA.mul(rA.mul(_tokenDecimalsOffsetA)).add(priceB.mul(rB.mul(_tokenDecimalsOffsetB))).div(totalSupply)
118        );
119        updatedAt = assetUpdatedAtA;
120
121        // use earlier time for updateAt
122        if (assetUpdatedAtA > assetUpdatedAtB) {
123            updatedAt = assetUpdatedAtB;
124        }
125    }
```

##### Recommendation

Do not use AMM pool or custom liquidity calculation to caculate LP token value/price.

## 2. MWE-200: Insecure LP Token Value Calculation

 High risk Security Analyzer

Liquidity token value/price can be manipulated to cause flashloan attacks.

### File(s) Affected



core/contracts/oracles/BalancerV2LPOracle.sol #88-124

```
88     function latestRoundData()
89     public
90     view
91     override
92     returns (
93         uint80 roundId,
94         int256 answer,
95         uint256 startedAt,
96         uint256 updatedAt,
97         uint80 answeredInRound
98     )
99     {
100         (address[] memory tokens, uint256[] memory balances, ) = vault.getPoolTokens(poolId);
101         (, int256 answerA, , uint256 assetUpdatedAtA, ) = oracleA.latestRoundData();
102         (, int256 answerB, , uint256 assetUpdatedAtB, ) = oracleB.latestRoundData();
103
104         uint256[] memory normalizedWeights = pool.getNormalizedWeights();
105
106         uint256 pxA = uint256(answerA);
107         uint256 pxB = uint256(answerB);
108         (uint256 fairResA, uint256 fairResB) = _computeFairReserves(
109             _getNormalizedBalance(tokens[0], balances[0]),
110             _getNormalizedBalance(tokens[1], balances[1]),
111             normalizedWeights[0],
112             normalizedWeights[1],
113             pxA,
114             pxB
115         );
116
117         answer = int256(fairResA.mul(pxA).add(fairResB.mul(pxB)).div(pool.totalSupply()));
118         updatedAt = assetUpdatedAtA;
119
120         // use oldest timestamp for updatedAt
121         if (assetUpdatedAtA > assetUpdatedAtB) {
122             updatedAt = assetUpdatedAtB;
123         }
124     }
```

### Recommendation

Do not use AMM pool or custom liquidity calculation to calculate LP token value/price.

### 3. MWE-200: Insecure LP Token Value Calculation

 High risk Security Analyzer

Liquidity token value/price can be manipulated to cause flashloan attacks.

#### File(s) Affected

core/contracts/liquidityMining/GenericMiner.sol #164-173

```
164     function _refresh() internal {
165         if (totalStake == 0) {
166             return;
167         }
168         uint256 currentBalance = a.mimo().balanceOf(address(this));
169         uint256 reward = currentBalance.sub(_balanceTracker);
170         _balanceTracker = currentBalance;
171
172         _accAmountPerShare = _accAmountPerShare.add(reward.rayDiv(totalStake));
173     }
```



core/contracts/liquidityMining/GenericMiner.sol #112-133

```
112     function _increaseStake(address user, uint256 value) internal {
113         require(value > 0, "STAKE_MUST_BE_GREATER_THAN_ZERO"); //TODO cleanup error message
114
115         UserInfo storage userInfo = _users[user];
116         _refresh();
117
118         uint256 pending;
119         if (userInfo.stake > 0) {
120             pending = userInfo.stake.rayMul(_accAmountPerShare.sub(userInfo.accAmountPerShare));
121             _balanceTracker = _balanceTracker.sub(pending);
122         }
123
124         totalStake = totalStake.add(value);
125         userInfo.stake = userInfo.stake.add(value);
126         userInfo.accAmountPerShare = _accAmountPerShare;
127
128         if (pending > 0) {
129             require(a.mimo().transfer(user, pending));
130         }
131
132         emit StakeIncreased(user, value);
133     }
```

#### Recommendation

Do not use AMM pool or custom liquidity calculation to calculate LP token value/price.

#### 4. MWE-200: Insecure LP Token Value Calculation

 High risk Security Analyzer

Liquidity token value/price can be manipulated to cause flashloan attacks.

##### File(s) Affected



core/contracts/liquidityMining/v2/PARMinerV2.sol #375-383

```
375 function _pendingMIMO(uint256 _userStakeWithBoost, uint256 _userAccAmountPerShare) internal view returns (uint256) {
376     if (_totalStakeWithBoost == 0) {
377         return 0;
378     }
379     uint256 currentBalance = _a.mimo().balanceOf(address(this));
380     uint256 reward = currentBalance.sub(_mimoBalanceTracker);
381     uint256 accMimoAmountPerShare = _accMimoAmountPerShare.add(reward.rayDiv(_totalStakeWithBoost));
382     return _userStakeWithBoost.rayMul(accMimoAmountPerShare.sub(_userAccAmountPerShare));
383 }
```

##### Recommendation

Do not use AMM pool or custom liquidity calculation to calculate LP token value/price.

#### 5. MWE-200: Insecure LP Token Value Calculation

 High risk Security Analyzer

Liquidity token value/price can be manipulated to cause flashloan attacks.

##### File(s) Affected

core/contracts/liquidityMining/v2/GenericMinerV2.sol #280-288

```
280 function _pendingMIMO(uint256 _userStakeWithBoost, uint256 _userAccAmountPerShare) internal view returns (uint256) {
281     if (_totalStakeWithBoost == 0) {
282         return 0;
283     }
284     uint256 currentBalance = _a.mimo().balanceOf(address(this));
285     uint256 reward = currentBalance.sub(_mimoBalanceTracker);
286     uint256 accMimoAmountPerShare = _accMimoAmountPerShare.add(reward.rayDiv(_totalStakeWithBoost));
287     return _userStakeWithBoost.rayMul(accMimoAmountPerShare.sub(_userAccAmountPerShare));
288 }
```

##### Recommendation

Do not use AMM pool or custom liquidity calculation to calculate LP token value/price.

#### Medium risk (0)

No Medium risk vulnerabilities found here

#### Low risk (0)

No Low risk vulnerabilities found here

#### 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 115-2022-04-mimo (StaticFail) (1Positive-FLP) 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 115-2022-04-mimo (StaticFail) (1Positive-FLP) 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.