








METATRUST

Draft  
Security Assessment for  
**77-2022-01-  
elasticswap  
(1Negative-FD)  
(1Positive-FLP)**

July 23, 2023






## Executive Summary

Overview			
Project Name	77-2022-01-elasticswap (1Negative-FD) (1Positive-FLP)	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.
Codebase URL	https://github.com/code-423n4/2022-01-elasticswap		
Scan Engine	AI Analyzer	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.
Scan Time	2023/07/23 02:01:57		
Commit Id	fc9b21	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.
			

Total	
Critical Issues	0
High risk Issues	1
Medium risk Issues	0
Low risk Issues	0
Informational Issues	0



	Critical Issues	0%	0
	High risk Issues	100%	1
	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 02:01:57** on project **77-2022-01-elasticswap (1Negative-FD) (1Positive-FLP)** with the repository **<https://github.com/code-423n4/2022-01-elasticswap>** 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 **1** vulnerabilities / security risks discovered during the scanning session, among which **0** critical vulnerabilities, **1** 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



## Findings

### Critical (0)

No Critical vulnerabilities found here

### High risk (1)

## 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

elasticswap/src/libraries/MathLib.sol #692-708

```
692     function calculateLiquidityTokenFees(  
693         uint256 _totalSupplyOfLiquidityTokens,  
694         InternalBalances memory _internalBalances  
695     ) public pure returns (uint256 liquidityTokenFeeQty) {  
696         uint256 rootK =  
697             sqrt(  
698                 _internalBalances.baseTokenReserveQty *  
699                 _internalBalances.quoteTokenReserveQty  
700             );  
701         uint256 rootKLast = sqrt(_internalBalances.kLast);  
702         if (rootK > rootKLast) {  
703             uint256 numerator =  
704                 _totalSupplyOfLiquidityTokens * (rootK - rootKLast);  
705             uint256 denominator = (rootK * 5) + rootKLast;  
706             liquidityTokenFeeQty = numerator / denominator;  
707         }  
708     }
```

elasticswap/src/libraries/MathLib.sol #378-513

```
378     function calculateAddLiquidityQuantities(  
379         uint256 _baseTokenQtyDesired,  
380         uint256 _quoteTokenQtyDesired,  
381         uint256 _baseTokenQtyMin,  
382         uint256 _quoteTokenQtyMin,  
383         uint256 _baseTokenReserveQty,  
384         uint256 _quoteTokenReserveQty,  
385         uint256 _totalSupplyOfLiquidityTokens,  
386         InternalBalances storage _internalBalances  
387     ) public returns (TokenQtys memory tokenQtys) {  
388         if (_totalSupplyOfLiquidityTokens > 0) {  
389             // we have outstanding liquidity tokens present and an existing price curve  
390  
391             tokenQtys.liquidityTokenFeeQty = calculateLiquidityTokenFees(  
392                 _totalSupplyOfLiquidityTokens,  
393                 _internalBalances  
394             );  
395  
396             // we need to take this amount (that will be minted) into account for below calculations  
397             _totalSupplyOfLiquidityTokens += tokenQtys.liquidityTokenFeeQty;  
398  
399             // confirm that we have no beta or alpha decay present  
400             // if we do, we need to resolve that first  
401             if (  
402                 isSufficientDecayPresent(  
403                     _baseTokenReserveQty,  
404                     _internalBalances  
405                 )  
406             ) {  
407                 // decay is present and needs to be dealt with by the caller.  
408  
409                 uint256 baseTokenQtyFromDecay;  
410                 uint256 quoteTokenQtyFromDecay;  
411                 uint256 liquidityTokenQtyFromDecay;  
412  
413                 if (  
414                     _baseTokenReserveQty > _internalBalances.baseTokenReserveQty  
415                 ) {  
416                     // we have more base token than expected (base token decay) due to rebase up  
417                     // we first need to handle this situation by requiring this user  
418                     // to add quote tokens  
419                     (  
420                         quoteTokenQtyFromDecay,  
421                         liquidityTokenQtyFromDecay  
422                     ) = calculateAddQuoteTokenLiquidityQuantities(  
423                         _quoteTokenQtyDesired,  
424                         0, // there is no minimum for this particular call since we may use quote tokens  
425                         _baseTokenReserveQty,  
426                         _totalSupplyOfLiquidityTokens,  
427                         _internalBalances  
428                     );  
429                 } else {  
430                     // we have less base token than expected (quote token decay) due to a rebase down  
431                     // we first need to handle this by adding base tokens to offset this.  
432                     (  
433                         baseTokenQtyFromDecay,  
434                         liquidityTokenQtyFromDecay
```

```
435         ) = calculateAddBaseTokenLiquidityQuantities(  
436             _baseTokenQtyDesired,  
437             0, // there is no minimum for this particular call since we may use base tokens  
438             _baseTokenReserveQty,  
439             _totalSupplyOfLiquidityTokens,  
440             _internalBalances  
441         );  
442     }  
443  
444     if (  
445         quoteTokenQtyFromDecay < _quoteTokenQtyDesired &&  
446         baseTokenQtyFromDecay < _baseTokenQtyDesired  
447     ) {  
448         // the user still has qty that they desire to contribute to the exchange for liquidity  
449         (  
450             tokenQtys.baseTokenQty,  
451             tokenQtys.quoteTokenQty,  
452             tokenQtys.liquidityTokenQty  
453         ) = calculateAddTokenPairLiquidityQuantities(  
454             _baseTokenQtyDesired - baseTokenQtyFromDecay, // safe from underflow quoted on  
455             _quoteTokenQtyDesired - quoteTokenQtyFromDecay, // safe from underflow quoted on  
456             0, // we will check minimums below  
457             0, // we will check minimums below  
458             _quoteTokenReserveQty + quoteTokenQtyFromDecay,  
459             _totalSupplyOfLiquidityTokens +  
460             liquidityTokenQtyFromDecay,  
461             _internalBalances // NOTE: these balances have already been updated when we did  
462         );  
463     }  
464     tokenQtys.baseTokenQty += baseTokenQtyFromDecay;  
465     tokenQtys.quoteTokenQty += quoteTokenQtyFromDecay;  
466     tokenQtys.liquidityTokenQty += liquidityTokenQtyFromDecay;  
467  
468     require(  
469         tokenQtys.baseTokenQty >= _baseTokenQtyMin,  
470         "MathLib: INSUFFICIENT_BASE_QTY"  
471     );  
472  
473     require(  
474         tokenQtys.quoteTokenQty >= _quoteTokenQtyMin,  
475         "MathLib: INSUFFICIENT_QUOTE_QTY"  
476     );  
477 } else {  
478     // the user is just doing a simple double asset entry / providing both base and quote.  
479     (  
480         tokenQtys.baseTokenQty,  
481         tokenQtys.quoteTokenQty,  
482         tokenQtys.liquidityTokenQty  
483     ) = calculateAddTokenPairLiquidityQuantities(  
484         _baseTokenQtyDesired,  
485         _quoteTokenQtyDesired,  
486         _baseTokenQtyMin,  
487         _quoteTokenQtyMin,  
488         _quoteTokenReserveQty,  
489         _totalSupplyOfLiquidityTokens,  
490         _internalBalances  
491     );  
492 }  
493 } else {
```

```
494 // this user will set the initial pricing curve
495 require (
496     _baseTokenQtyDesired > 0,
497     "MathLib: INSUFFICIENT_BASE_QTY_DESIRED"
498 );
499 require (
500     _quoteTokenQtyDesired > 0,
501     "MathLib: INSUFFICIENT_QUOTE_QTY_DESIRED"
502 );
503
504 tokenQtys.baseTokenQty = _baseTokenQtyDesired;
505 tokenQtys.quoteTokenQty = _quoteTokenQtyDesired;
506 tokenQtys.liquidityTokenQty = sqrt (
507     _baseTokenQtyDesired * _quoteTokenQtyDesired
508 );
509
510 _internalBalances.baseTokenReserveQty += tokenQtys.baseTokenQty;
511 _internalBalances.quoteTokenReserveQty += tokenQtys.quoteTokenQty;
512 }
513 }
```

#### 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 77-2022-01-elasticswap (1Negative-FD) (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 77-2022-01-elasticswap (1Negative-FD) (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.