



METATRUST

Draft
Security Assessment for
**78-2022-01-behodler
(10K-FLP) (1Positive-
ANC)**

July 24, 2023






Executive Summary

Overview			
Project Name	78-2022-01-behodler (1OK-FLP) (1Positive-ANC)		
Codebase URL	https://github.com/code-423n4/2022-01-behodler		
Scan Engine	AI Analyzer		
Scan Time	2023/07/24 02:05:31		
Commit Id	71bc7f3		

Total			
Critical Issues	0		
High risk Issues	6		
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%	6
	Medium risk Issues	0%	0
	Low risk Issues	0%	0
	Informational Issues	0%	0

Summary of Findings

MetaScan security assessment was performed on **July 24, 2023 02:05:31** on project **78-2022-01-behodler (1OK-FLP) (1Positive-ANC)** with the repository <https://github.com/code-423n4/2022-01-behodler> 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 **6** vulnerabilities / security risks discovered during the scanning session, among which **0** critical vulnerabilities, **6** 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-203: Approval Not Revoked	High risk
MSA-006	MWE-203: Approval Not Revoked	High risk


Findings

Critical (0)

No Critical vulnerabilities found here

High risk (6)

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

contracts/UniswapHelper.sol #147-157

```
147     function getLatestFLNQuote() internal view returns (uint256 dai_scx, uint256 daiBalanceOnBehodler) {
148         uint256 daiToRelease = BehodlerLike(VARS.behodler).withdrawLiquidityFindSCX(
149             VARS.DAI,
150             10000,
151             1 ether,
152             VARS.precision
153         );
154         dai_scx = (daiToRelease * EXA) / (1 ether);
155
156         daiBalanceOnBehodler = IERC20(VARS.DAI).balanceOf(VARS.behodler);
157     }
```



contracts/UniswapHelper.sol #138-145

```
138     function generateFLNQuote() public override {
139         latestFlanQuotes[1] = latestFlanQuotes[0];
140         (
141             latestFlanQuotes[0].DaiScxSpotPrice,
142             latestFlanQuotes[0].DaiBalanceOnBehodler
143         ) = getLatestFLNQuote();
144         latestFlanQuotes[0].blockProduced = block.number;
145     }
```

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



contracts/UniswapHelper.sol #217-235

```
217     function buyFlanAndBurn(  
218         address inputToken,  
219         uint256 amount,  
220         address recipient  
221     ) public override {  
222         address pair = VARS.factory.getPair(inputToken, VARS.flan);  
223  
224         uint256 flanBalance = IERC20(VARS.flan).balanceOf(pair);  
225         uint256 inputBalance = IERC20(inputToken).balanceOf(pair);  
226  
227         uint256 amountOut = getAmountOut(amount, inputBalance, flanBalance);  
228         uint256 amount0Out = inputToken < VARS.flan ? 0 : amountOut;  
229         uint256 amount1Out = inputToken < VARS.flan ? amountOut : 0;  
230         IERC20(inputToken).transfer(pair, amount);  
231         UniPairLike(pair).swap(amount0Out, amount1Out, address(this), "");  
232         uint256 reward = (amountOut / 100);  
233         ERC20Burnable(VARS.flan).transfer(recipient, reward);  
234         ERC20Burnable(VARS.flan).burn(amountOut - reward);  
235     }
```

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

contracts/TokenProxies/RebaseProxy.sol #19-24

```
19     function redeemRate() public view returns (uint256) {
20         uint256 balanceOfBase = IERC20(baseToken).balanceOf(address(this));
21         if (totalSupply() == 0 || balanceOfBase == 0) return ONE;
22
23         return (balanceOfBase * ONE) / totalSupply();
24     }
```



contracts/TokenProxies/RebaseProxy.sol #26-38

```
26     function mint(address to, uint256 amount)
27     public
28     override
29     returns (uint256)
30     {
31         uint256 _redeemRate = redeemRate();
32         require(
33             IERC20(baseToken).transferFrom(msg.sender, address(this), amount)
34         );
35         uint256 baseBalance = IERC20(baseToken).balanceOf(address(this));
36         uint256 proxy = (baseBalance * ONE) / _redeemRate;
37         _mint(to, proxy);
38     }
```

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

contracts/TokenProxies/RebaseProxy.sol #26-38

```
26     function mint(address to, uint256 amount)
27     public
28     override
29     returns (uint256)
30     {
31         uint256 _redeemRate = redeemRate();
32         require(
33             IERC20(baseToken).transferFrom(msg.sender, address(this), amount)
34         );
35         uint256 baseBalance = IERC20(baseToken).balanceOf(address(this));
36         uint256 proxy = (baseBalance * ONE) / _redeemRate;
37         _mint(to, proxy);
38     }
```



contracts/UniswapHelper.sol #162-197

```
162 function stabilizeFlan(uint256 rectangleOfFairness) public override onlyLimbo ensurePriceStability re
163     uint256 localSCXBalance = IERC20(VARS.behodler).balanceOf(address(this));
164
165     //SCX transfers incur a 2% fee. Checking that SCX balance == rectangleOfFairness must take this in
166     //Note that for hardcoded values, this contract can be upgraded through governance so we're not ig
167     require((localSCXBalance * 100) / rectangleOfFairness == 98, "EM");
168     rectangleOfFairness = localSCXBalance;
169
170     //get DAI per scx
171     uint256 existingSCXBalanceOnLP = IERC20(VARS.behodler).balanceOf(address(VARS.Flan_SCX_tokenPair));
172     uint256 finalSCXBalanceOnLP = existingSCXBalanceOnLP + rectangleOfFairness;
173
174     //the DAI value of SCX is the final quantity of Flan because we want Flan to hit parity with Dai.
175     uint256 DesiredFinalFlanOnLP = ((finalSCXBalanceOnLP * latestFlanQuotes[0].DaiScxSpotPrice) / EXA);
176     address pair = address(VARS.Flan_SCX_tokenPair);
177     uint256 existingFlanOnLP = IERC20(VARS.flan).balanceOf(pair);
178
179     if (existingFlanOnLP < DesiredFinalFlanOnLP) {
180         uint256 flanToMint = ((DesiredFinalFlanOnLP - existingFlanOnLP) * (100 - VARS.priceBoostOvershoot
181
182         flanToMint = flanToMint == 0 ? DesiredFinalFlanOnLP - existingFlanOnLP : flanToMint;
183         FlanLike(VARS.flan).mint(pair, flanToMint);
184         IERC20(VARS.behodler).transfer(pair, rectangleOfFairness);
185         {
186             lpMinted = VARS.Flan_SCX_tokenPair.mint(VARS.blackHole);
187         }
188     } else {
189         uint256 minFlan = existingFlanOnLP / VARS.Flan_SCX_tokenPair.totalSupply();
190
191         FlanLike(VARS.flan).mint(pair, minFlan + 2);
192         IERC20(VARS.behodler).transfer(pair, rectangleOfFairness);
193         lpMinted = VARS.Flan_SCX_tokenPair.mint(VARS.blackHole);
194     }
195     //Don't allow future migrations to piggy back off the data collected by recent migrations. Forces a
196     _zeroOutQuotes();
197 }
```

Recommendation

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

5. MWE-203: Approval Not Revoked

 High risk Security Analyzer

Approval is not revoked or reset after the code functionality finishes.

File(s) Affected



contracts/DAO/LimboDAO.sol #323-372

```
323     function setEYEBasedAssetStake(  
324         uint256 finalAssetBalance,  
325         uint256 finalEYEBalance,  
326         uint256 rootEYE,  
327         address asset  
328     ) public isLive incrementFate {  
329         require(assetApproved[asset], "LimboDAO: illegal asset");  
330         address sender = _msgSender();  
331         FateGrowthStrategy strategy = fateGrowthStrategy[asset];  
332  
333         //verifying that rootEYE value is accurate within precision.  
334         uint256 rootEYESquared = rootEYE * rootEYE;  
335         uint256 rootEYEPlusOneSquared = (rootEYE + 1) * (rootEYE + 1);  
336         require(  
337             rootEYESquared <= finalEYEBalance && rootEYEPlusOneSquared > finalEYEBalance,  
338             "LimboDAO: Stake EYE invariant."  
339         );  
340         AssetClout storage clout = stakedUserAssetWeight[sender][asset];  
341         fateState[sender].fatePerDay -= clout.fateWeight;  
342         uint256 initialBalance = clout.balance;  
343         //EYE  
344         if (strategy == FateGrowthStrategy.directRoot) {  
345             require(finalAssetBalance == finalEYEBalance, "LimboDAO: staking eye invariant.");  
346             require(asset == domainConfig.eye);  
347  
348             clout.fateWeight = rootEYE;  
349             clout.balance = finalAssetBalance;  
350             fateState[sender].fatePerDay += rootEYE;  
351         } else if (strategy == FateGrowthStrategy.indirectTwoRootEye) {  
352             //LP  
353             clout.fateWeight = 2 * rootEYE;  
354             fateState[sender].fatePerDay += clout.fateWeight;  
355  
356             uint256 actualEyeBalance = IERC20(domainConfig.eye).balanceOf(asset);  
357             require(actualEyeBalance > 0, "LimboDAO: No EYE");  
358             uint256 totalSupply = IERC20(asset).totalSupply();  
359             uint256 eyePerUnit = (actualEyeBalance * ONE) / totalSupply;  
360             uint256 impliedEye = (eyePerUnit * finalAssetBalance) / (ONE * precision);  
361             finalEYEBalance /= precision;  
362             require(  
363                 finalEYEBalance == impliedEye, //precision cap  
364                 "LimboDAO: stake invariant check 2."  
365             );  
366             clout.balance = finalAssetBalance;  
367         } else {  
368             revert("LimboDAO: asset growth strategy not accounted for");  
369         }  
370         int256 netBalance = int256(finalAssetBalance) - int256(initialBalance);  
371         asset.ERC20NetTransfer(sender, address(this), netBalance);  
372     }
```

Recommendation

Try to remove the approval after the code finishes its job.

6. MWE-203: Approval Not Revoked

 **High risk**
 **Security Analyzer**

Approval is not revoked or reset after the code functionality finishes.

File(s) Affected

contracts/DAO/LimboDAO.sol #383-401

```

383 function burnAsset(address asset, uint256 amount) public isLive incrementFate {
384     require(assetApproved[asset], "LimboDAO: illegal asset");
385     address sender = _msgSender();
386     require(ERC677(asset).transferFrom(sender, address(this), amount), "LimboDAO: transferFailed");
387     uint256 fateCreated = fateState[_msgSender()].fateBalance;
388     if (asset == domainConfig.eye) {
389         fateCreated = amount * 10;
390         ERC677(domainConfig.eye).burn(amount);
391     } else {
392         uint256 actualEyeBalance = IERC20(domainConfig.eye).balanceOf(asset);
393         require(actualEyeBalance > 0, "LimboDAO: No EYE");
394         uint256 totalSupply = IERC20(asset).totalSupply();
395         uint256 eyePerUnit = (actualEyeBalance * ONE) / totalSupply;
396         uint256 impliedEye = (eyePerUnit * amount) / ONE;
397         fateCreated = impliedEye * 20;
398     }
399     fateState[_msgSender()].fateBalance += fateCreated;
400     emit assetBurnt(_msgSender(), asset, fateCreated);
401 }

```

Recommendation

Try to remove the approval after the code finishes its job.

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 78-2022-01-behodler (1OK-FLP) (1Positive-ANC) 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 78-2022-01-behodler (1OK-FLP) (1Positive-ANC) 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.