



METATRUST

Draft

Security Assessment for






59-2021-11-malt (10K- FLB) (1Positive-FLP)

July 23, 2023

Executive Summary

Overview			
Project Name	59-2021-11-malt (1OK-FLB) (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-423n4/2021-11-malt		
Scan Engine	AI Analyzer		
Scan Time	2023/07/23 01:45:54	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.
Commit Id	55b7dc6		
Total		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.
Critical Issues	0		
High risk Issues	5	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.
Medium risk Issues	0		
Low risk Issues	0	Informational Issue	The issue does not pose an immediate risk but is relevant to security best practices or Defence in Depth.
Informational Issues	0		



	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 01:45:54** on project **59-2021-11-malt (10K-FLB) (1Positive-FLP)** with the repository <https://github.com/code-423n4/2021-11-malt> 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-202: Insecure Token Buying Behavior	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



src/contracts/ImpliedCollateralService.sol #104-115

```
104     function getCollateralValueInMalt() public view returns (uint256 collateral) {
105         uint256 maltPrice = maltDataLab.smoothedMaltPrice();
106         uint256 target = maltDataLab.priceTarget();
107
108         uint256 auctionPoolBalance = collateralToken.balanceOf(address(auctionPool)).mul(target).div(maltPrice);
109         uint256 overflowBalance = collateralToken.balanceOf(address(rewardOverflow)).mul(target).div(maltPrice);
110         uint256 liquidityExtensionBalance = collateralToken.balanceOf(address(liquidityExtension)).mul(target).div(maltPrice);
111         uint256 swingTraderBalance = collateralToken.balanceOf(address(swingTrader)).mul(target).div(maltPrice);
112         uint256 swingTraderMaltBalance = malt.balanceOf(address(swingTrader));
113
114         return auctionPoolBalance + overflowBalance + liquidityExtensionBalance + swingTraderBalance + swingTraderMaltBalance;
115     }
```

Recommendation

Do not use AMM pool or custom liquidity calculation to calculate 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



src/contracts/MaltDataLab.sol #133-151

```
133     function trackMaltPrice()
134     external
135     onlyRole(UPDATER_ROLE, "Must have updater role")
136     {
137         (uint256 reserve0, uint256 reserve1,) = stakeToken.getReserves();
138         (address token0,) = UniswapV2Library.sortTokens(address(malt), address(rewardToken));
139         uint256 rewardDecimals = rewardToken.decimals();
140
141         if (token0 == address(rewardToken)) {
142             uint256 price = _normalizedPrice(reserve0, reserve1, rewardDecimals);
143             maltPriceMA.update(price);
144             emit TrackMaltPrice(price);
145         } else {
146             uint256 price = _normalizedPrice(reserve1, reserve0, rewardDecimals);
147             maltPriceMA.update(price);
148
149             emit TrackMaltPrice(price);
150         }
151     }
```

Recommendation

Do not use AMM pool or custom liquidity calculation to caculate 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



src/contracts/DexHandlers/UniswapHandler.sol #80-109

```
80  function maltMarketPrice() public view returns (uint256 price, uint256 decimals) {
81      // TODO use datalab anywhere that calls this Tue 05 Oct 2021 20:56:41 BST
82      (uint256 maltReserves, uint256 rewardReserves) = UniswapV2Library.getReserves(
83          uniswapV2Factory,
84          address(malt),
85          address(rewardToken)
86      );
87
88      if (maltReserves == 0 || rewardReserves == 0) {
89          price = 0;
90          decimals = 18;
91          return (price, decimals);
92      }
93
94      uint256 rewardDecimals = rewardToken.decimals();
95      uint256 maltDecimals = malt.decimals();
96
97      if (rewardDecimals > maltDecimals) {
98          uint256 diff = rewardDecimals - maltDecimals;
99          price = rewardReserves.mul(10**rewardDecimals).div(maltReserves.mul(10**diff));
100         decimals = rewardDecimals;
101     } else if (rewardDecimals < maltDecimals) {
102         uint256 diff = maltDecimals - rewardDecimals;
103         price = (rewardReserves.mul(10**diff)).mul(10**rewardDecimals).div(maltReserves);
104         decimals = maltDecimals;
105     } else {
106         price = rewardReserves.mul(10**rewardDecimals).div(maltReserves);
107         decimals = rewardDecimals;
108     }
109 }
```

Recommendation

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

4. MWE-202: Insecure Token Buying Behavior

 High risk Security Analyzer

Buying tokens via swap or AMM can be manipulated to cause sandwich attacks.

File(s) Affected



src/contracts/DexHandlers/UniswapHandler.sol #131-158

```
131 function buyMalt()
132     external
133     onlyRole(BUYER_ROLE, "Must have buyer privs")
134     returns (uint256 purchased)
135 {
136     uint256 rewardBalance = rewardToken.balanceOf(address(this));
137
138     if (rewardBalance == 0) {
139         return 0;
140     }
141
142     rewardToken.approve(address(router), rewardBalance);
143
144     address[] memory path = new address[](2);
145     path[0] = address(rewardToken);
146     path[1] = address(malt);
147
148     router.swapExactTokensForTokens(
149         rewardBalance,
150         0, // amountOutMin
151         path,
152         address(this),
153         now
154     );
155
156     purchased = malt.balanceOf(address(this));
157     malt.safeTransfer(msg.sender, purchased);
158 }
```

Recommendation

Do not use swap or AMM to buy tokens.

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

src/contracts/libraries/UniswapV2Library.sol #29-33

```
29     function getReserves(address factory, address tokenA, address tokenB) internal view returns (uint re
30         (address token0,) = sortTokens(tokenA, tokenB);
31         (uint reserve0, uint reserve1,) = IUniswapV2Pair(pairFor(factory, tokenA, tokenB)).getReserves()
32         (reserveA, reserveB) = tokenA == token0 ? (reserve0, reserve1) : (reserve1, reserve0);
33     }
```

src/contracts/libraries/UniswapV2Library.sol #62-70

```
62     function getAmountsOut(address factory, uint amountIn, address[] memory path) internal view returns
63         require(path.length >= 2, 'UniswapV2Library: INVALID_PATH');
64         amounts = new uint[](path.length);
65         amounts[0] = amountIn;
66         for (uint i; i < path.length - 1; i++) {
67             (uint reserveIn, uint reserveOut) = getReserves(factory, path[i], path[i + 1]);
68             amounts[i + 1] = getAmountOut(amounts[i], reserveIn, reserveOut);
69         }
70     }
```

Recommendation

Do not use AMM pool or custom liquidity calculation to caculate 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 59-2021-11-malt (1OK-FLB) (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 59-2021-11-malt (1OK-FLB) (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.