



METATRUST






Draft
Security Assessment for
**Hack-20220321-
OneRingFinance (10K-
FLP)**

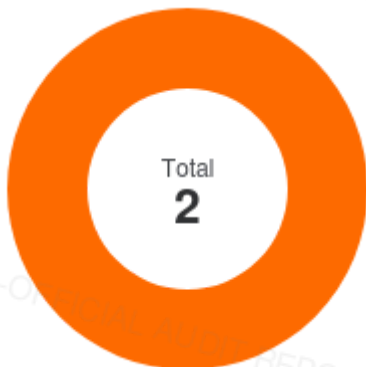
July 23, 2023






Executive Summary

Overview			
Project Name	Hack-20220321-OneRingFinance (1OK-FLP)		
Codebase URL	-		
Scan Engine	AI Analyzer		
Scan Time	2023/07/23 15:11:41		
Commit Id	-		

Total			
Critical Issues	0		
High risk Issues	2		
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%	2
	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 15:11:41** on project **Hack-20220321-OneRingFinance (10K-FLP)** with the repository **Hack_20220321_OneRingFinance** 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 **2** vulnerabilities / security risks discovered during the scanning session, among which **0** critical vulnerabilities, **2** 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



Findings

Critical (0)

No Critical vulnerabilities found here

High risk (2)

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/strategies/base/MasterChefBaseStrategy.sol #175-204

```
175     function _assetFromUnderlying(  
176         address _asset,  
177         uint256 _liquidity,  
178         address[] memory _route0,  
179         address[] memory _route1  
180     ) internal {  
181         address _token0 = IUniswapV2Pair(underlying).token0();  
182         address _token1 = IUniswapV2Pair(underlying).token1();  
183  
184         IUniswapV2Router02(router).removeLiquidity(  
185             _token0,  
186             _token1,  
187             _liquidity,  
188             1, // we are willing to take whatever the pair gives us  
189             1, // we are willing to take whatever the pair gives us  
190             address(this),  
191             block.timestamp  
192         );  
193  
194         uint256 _token0Amount = IERC20(_token0).balanceOf(address(this));  
195         uint256 _token1Amount = IERC20(_token1).balanceOf(address(this));  
196  
197         if (_route0.length > 1) {  
198             _swapSushiswapWithPath(_route0, _token0Amount);  
199         }  
200  
201         if (_route1.length > 1) {  
202             _swapSushiswapWithPath(_route1, _token1Amount);  
203         }  
204     }
```



contracts/strategies/base/MasterChefBaseStrategy.sol #255-302

```
255     function withdrawToVault(uint256 _usdAmount, address _asset)
256     external
257     restricted
258     {
259         address _token0 = IUniswapV2Pair(underlying).token0();
260         address _token1 = IUniswapV2Pair(underlying).token1();
261         uint256 _usdBal = getUSDBalanceFromUnderlyingBalance(
262             underlyingBalance()
263         );
264
265         if (_usdBal == 0) {
266             return;
267         }
268
269         uint256 _defaultUnit = uint256(10)**uint256(18);
270         uint256 _assetUnit = uint256(10)**uint256(ERC20(_asset).decimals());
271
272         uint256 _underlyingBal = IERC20(underlying).balanceOf(address(this));
273
274         uint256 _amount = underlyingBalance().mul(_usdAmount).div(_usdBal);
275
276         if (_amount < _underlyingBal) {
277             uint256 _toWithdraw = _amount.mul(_assetUnit).div(_defaultUnit);
278
279             IERC20(_asset).safeTransferFrom(address(this), vault, _toWithdraw);
280
281             return;
282         }
283
284         uint256 _missing = _amount.sub(_underlyingBal);
285         if (_missing > rewardPoolUnderlyingBalance()) {
286             _missing = rewardPoolUnderlyingBalance();
287         }
288
289         IMasterChef(masterChef).withdraw(poolId, _missing);
290
291         _assetFromUnderlying(
292             _asset,
293             _missing,
294             toVaultAssetRoutes[_asset][_token0],
295             toVaultAssetRoutes[_asset][_token1]
296         );
297
298         IERC20(_asset).safeTransfer(
299             vault,
300             IERC20(_asset).balanceOf(address(this))
301         );
302     }
```

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

contracts/strategies/base/MasterChefBaseStrategy.sol #378-406

```

378     function getUSDBalanceFromUnderlyingBalance(uint256 _bal)
379         public
380         view
381         returns (uint256 _amount)
382     {
383         if (_bal > 0) {
384             address _token0 = IUniswapV2Pair(underlying).token0();
385             address _token1 = IUniswapV2Pair(underlying).token1();
386
387             (uint256 _reserves0, uint256 _reserves1, ) = IUniswapV2Pair(
388                 underlying
389             ).getReserves();
390             uint256 _totalSupply = IERC20(underlying).totalSupply();
391
392             uint256 _amount0 = _reserves0.mul(_bal).div(_totalSupply);
393             uint256 _amount1 = _reserves1.mul(_bal).div(_totalSupply);
394
395             uint256 _vaultDecimals = ERC20(vault).decimals();
396             uint256 _vaultUnit = uint256(10)**uint256(_vaultDecimals);
397             uint256 _token0Unit = uint256(10) **
398                 uint256(ERC20(_token0).decimals());
399             uint256 _token1Unit = uint256(10) **
400                 uint256(ERC20(_token1).decimals());
401
402             _amount =
403                 _amount0.mul(_vaultUnit).div(_token0Unit) +
404                 _amount1.mul(_vaultUnit).div(_token1Unit);
405         }
406     }

```

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

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 Hack-20220321-OneRingFinance (1OK-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 Hack-20220321-OneRingFinance (1OK-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.