METATRUST

Draft
Security Assessment for

12-2021-05-yield (1OK-FLP) (1Positive-FD)

July 23, 2023

Executive Summary

Overview	
Project Name	12-2021-05-yield (1OK-FLP) (1Positive-FD)
Codebase URL	https://github.com/code-423n4/2021-05-yield
Scan Engine	AI Analyzer
Scan Time	2023/07/23 16:42:38
Commit Id	e4c8491

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 16:42:38** on project **12-2021-05-yield (1OK-FLP) (1Positive-FD)** with the repository **https://github.com/code-423n4/2021-05-yield** 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-204: Unsafe First Deposit	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-204: Unsafe First Deposit

High risk | Security Analyzer

First depositor can break minting of shares or drain the liquidity of all users.

File(s) Affected

contracts/yieldspace/Pool.sol #231-298

```
231     function _mintInternal(address to, bool calculateFromBase, uint256 fyTokenToBuy, uint256 minTokensM
232         internal
233         returns (uint256, uint256, uint256)
234     {
235         // Gather data
236         uint256 supply = _totalSupply;
237         (uint112 _baseCached, uint112 _fyTokenCached) =
238             (baseCached, fyTokenCached);
239         uint256 _realFYTokenCached = _fyTokenCached - supply;    // The fyToken cache includes the virt
240 
241         // Calculate trade
242         uint256 tokensMinted;
243         uint256 baseIn;
244         uint256 baseReturned;
245         uint256 fyTokenIn;
246 
247         if (supply == 0) {
248             require (calculateFromBase && fyTokenToBuy == 0, "Pool: Initialize only from base");
249             baseIn = base.balanceOf(address(this)) - _baseCached;
250             tokensMinted = baseIn;    // If supply == 0 we are initializing the pool and tokensMinted =
251         } else {
252             // There is an optional virtual trade before the mint
253             uint256 baseToSell;
254             if (fyTokenToBuy > 0) {     // calculateFromBase == true and fyTokenToBuy > 0 can't happen
255                 baseToSell = _buyFYTokenPreview(
256                     fyTokenToBuy.u128(),
257                     _baseCached,
258                     _fyTokenCached
259                 );
260             }
261 
262             if (calculateFromBase) {    // We use all the available base tokens, surplus is in fyTokens
263                 baseIn = base.balanceOf(address(this)) - _baseCached;
264                 tokensMinted = (supply * baseIn) / _baseCached;
265                 fyTokenIn = (_realFYTokenCached * tokensMinted) / supply;
266                 require(_realFYTokenCached + fyTokenIn <= fyToken.balanceOf(address(this)), "Pool: Not
267             } else {                    // We use all the available fyTokens, plus a virtual trade if it
268                 fyTokenIn = fyToken.balanceOf(address(this)) - _realFYTokenCached;
269                 tokensMinted = (supply * (fyTokenToBuy + fyTokenIn)) / (_realFYTokenCached - fyTokenToB
270                 baseIn = baseToSell + ((_baseCached + baseToSell) * tokensMinted) / supply;
271                 uint256 _baseBalance = base.balanceOf(address(this));
272                 require(_baseBalance - _baseCached >= baseIn, "Pool: Not enough base token in");
273 
274                 // If we did a trade means we came in through `mintWithBase`, and want to return the ba
275                 if (fyTokenToBuy > 0) baseReturned = (_baseBalance - _baseCached) - baseIn;
276             }
277         }
278 
279         // Slippage
280         require (tokensMinted >= minTokensMinted, "Pool: Not enough tokens minted");
281 
282         // Update TWAR
283         _update(
284             (_baseCached + baseIn).u128(),
285             (_fyTokenCached + fyTokenIn + tokensMinted).u128(), // Account for the "virtual" fyToken fr
286             _baseCached,
287             _fyTokenCached
```

```
288         );
289
290         // Execute mint
291         _mint(to, tokensMinted);
292
293         // Return any unused base if we did a trade, meaning slippage was involved.
294         if (supply > 0 && fyTokenToBuy > 0) base.safeTransfer(to, baseReturned);
295
296         emit Liquidity(maturity, msg.sender, to, -(baseIn.i256()), -(fyTokenIn.i256()), tokensMinted.i
297         return (baseIn, fyTokenIn, tokensMinted);
298     }
```

Recommendation

When totalSupply() == 0, send the first min liquidity LP tokens to the zero address to enable share dilution.

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/oracles/compound/CompoundMultiOracle.sol #40-53

```
40      function _peek(bytes6 base, bytes6 kind) private view returns (uint price, uint updateTime) {
41          uint256 rawPrice;
42          address source = sources[base][kind];
43          require (source != address(0), "Source not found");
44
45          if (kind == "rate") rawPrice = CTokenInterface(source).borrowIndex();
46          else if (kind == "chi") rawPrice = CTokenInterface(source).exchangeRateStored();
47          else revert("Unknown oracle type");
48
49          require(rawPrice > 0, "Compound price is zero");
50
51          price = rawPrice * SCALE_FACTOR;
52          updateTime = block.timestamp;
53      }
```

contracts/oracles/compound/CompoundMultiOracle.sol #69-73

```
69      function get(bytes32 base, bytes32 kind, uint256 amount) public virtual override view returns (uint2
70          uint256 price;
71          (price, updateTime) = _peek(base.b6(), kind.b6());
72          value = price * amount / 1e18;
73      }
```

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 12-2021-05-yield (1OK-FLP) (1Positive-FD) 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 12-2021-05-yield (1OK-FLP) (1Positive-FD) 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.