



METATRUST

Pre Report for
Derpdex-core

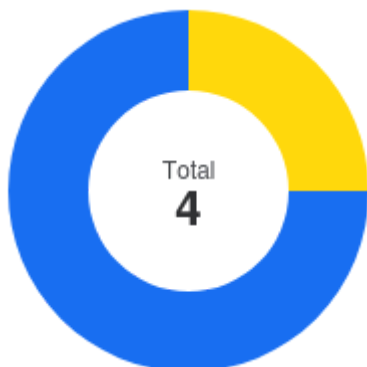
August 1, 2023






Executive Summary

Overview			
Project Name	Derpdex-core		
Codebase URL	https://github.com/derpdex-official/derpdex-core		
Scan Engine	Security Analyzer		
Scan Time	2023/08/1 16:11:27		
Commit Id	233a1d58		

Total	
Critical Issues	0
High risk Issues	0
Medium risk Issues	1
Low risk Issues	0
Informational Issues	3

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	0%	0
	Medium risk Issues	25%	1
	Low risk Issues	0%	0
	Informational Issues	75%	3

Summary of Findings

MetaScan security assessment was performed on **August 1, 2023 16:11:27** on project **Derpdex-core** with the repository <https://github.com/derpdex-official/derpdex-core> on branch **master**. The assessment was carried out by scanning the project's codebase using the scan engine **Security Analyzer**. There are in total **4** vulnerabilities / security risks discovered during the scanning session, among which **0** critical vulnerabilities, **0** high risk vulnerabilities, **1** medium risk vulnerabilities, **0** low risk vulnerabilities, **3** informational issues.

ID	Description	Severity
MSA-001	Centralized Role	Medium risk
MSA-002	Missing Error Message	Informational
MSA-003	Unnecessary Public Function Modifier	Informational
MSA-004	The Tickspacing is small	Informational

Findings

Critical (0)


No Critical vulnerabilities found here


High risk (0)

No High risk vulnerabilities found here

Medium risk (1)

1. Centralized Role

 Medium risk

 Security Analyzer

In the `UniswapV3Factory` contract, the privileged role `owner` has the privilege of the below function:

- `setOwner`: updates the owner of the factory;
- `enableFeeAmount`: enables a fee amount with the given tickSpacing.

In the `UniswapV3Pool` contract, the privileged role factory owner has the privilege of the below function:

- `setFeeProtocol`: sets the denominator of the protocol's % share of the fees;
- `collectProtocol`: collects the protocol fee accrued to the pool

File(s) Affected

contracts/UniswapV3Factory.sol #63-74



```
63     function enableFeeAmount(uint24 fee, int24 tickSpacing) public override {
64         require(msg.sender == owner);
65         require(fee < 1000000);
66         // tick spacing is capped at 16384 to prevent the situation where tickSpacing is so large that
67         // TickBitmap#nextInitializedTickWithinOneWord overflows int24 container from a valid tick
68         // 16384 ticks represents a >5x price change with ticks of 1 bips
69         require(tickSpacing > 0 && tickSpacing < 16384);
70         require(feeAmountTickSpacing[fee] == 0);
71
72         feeAmountTickSpacing[fee] = tickSpacing;
73         emit FeeAmountEnabled(fee, tickSpacing);
74     }
```

Low risk (0)

No Low risk vulnerabilities found here

Informational (3)

1. Missing Error Message

 Informational Security Analyzer

`require` can be used to check for conditions and throw an exception if the condition is not met, in which case the error message provided by the developer will appear. This is why a very descriptive error message is needed.

File(s) Affected

contracts/UniswapV3Pool.sol #143-143

```
143         require(success && data.length >= 32);
```

contracts/UniswapV3Pool.sol #153-153

```
153         require(success && data.length >= 32);
```

contracts/UniswapV3Pool.sol #188-188

```
188         require(initializedLower);
```

contracts/UniswapV3Pool.sol #197-197

```
197         require(initializedUpper);
```



contracts/UniswapV3Pool.sol #464-464

```
464         require(amount > 0);
```

Recommendation

Adding an error message describing all the failed condition.

2. Unnecessary Public Function Modifier

 Informational Security Analyzer

There are some public functions which can be replaced as external functions.

File(s) Affected

contracts/UniswapV3Factory.sol #63-74

```
63     function enableFeeAmount(uint24 fee, int24 tickSpacing) public override {
64         require(msg.sender == owner);
65         require(fee < 1000000);
66         // tick spacing is capped at 16384 to prevent the situation where tickSpacing is so large that
67         // TickBitmap#nextInitializedTickWithinOneWord overflows int24 container from a valid tick
68         // 16384 ticks represents a >5x price change with ticks of 1 bips
69         require(tickSpacing > 0 && tickSpacing < 16384);
70         require(feeAmountTickSpacing[fee] == 0);
71
72         feeAmountTickSpacing[fee] = tickSpacing;
73         emit FeeAmountEnabled(fee, tickSpacing);
74     }
```

contracts/MultiCall.sol #19-21

```
19     function getCurrentBlockTimestamp() public view returns (uint256 timestamp) {
20         timestamp = block.timestamp;
21     }
```

contracts/MultiCall.sol #23-25



```
23     function getEthBalance(address addr) public view returns (uint256 balance) {
24         balance = addr.balance;
25     }
```

contracts/MultiCall.sol #27-38

```
27     function multicall(Call[] memory calls) public returns (uint256 blockNumber, Result[] memory returnD
28         blockNumber = block.number;
29         returnData = new Result[](calls.length);
30         for (uint256 i = 0; i < calls.length; i++) {
31             (address target, uint256 gasLimit, bytes memory callData) =
32                 (calls[i].target, calls[i].gasLimit, calls[i].callData);
33             uint256 gasLeftBefore = gasleft();
34             (bool success, bytes memory ret) = target.call{gas: gasLimit}(callData);
35             uint256 gasUsed = gasLeftBefore - gasleft();
36             returnData[i] = Result(success, gasUsed, ret);
37         }
38     }
```

Recommendation

Consider replacing public with external

3. The Tickspacing is small Informational Security Analyzer

The `feeAmountTickSpacing` stands for the tick spacing for a given fee amount. As it is mentioned in the [white paper of Uniswap V3](#):

Small choices for tickSpacing allow tighter and more precise ranges, but may cause swaps to be more gas-intensive (since each initialized tick that a swap crosses imposes a gas cost on the swapper).

Tickspacing 1 is might too small for the fee amount 100.

File(s) Affected

contracts/UniswapV3Factory.sol #26-27

```
26         feeAmountTickSpacing[100] = 1;
27         emit FeeAmountEnabled(100, 1);
```

Recommendation

Consider enlarging the tickspacing of the fee amount 100, like 2.

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 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 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.