METATRUST

Security Assessment for

KTX Finance

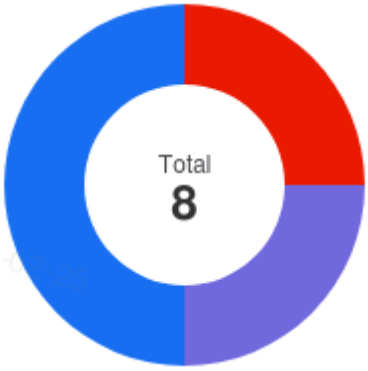
February 25, 2023

Executive Summary

Overview	
Project Name	KTX-core/
Codebase Path	git://github.com/https://github.com/KTX-finance/KTX-core/
Scan Engine	Security Analyzer
Scan Time	2023/02/25 21:35:26
Source Code	https://github.com/KTX-finance/KTX-core/ commit:b882729

Total	
Critical Issues	2
High risk Issues	0
Medium risk Issues	0
Low risk Issues	2
Informational Issues	4

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	25%	2
High risk Issues	0%	0
Medium risk Issues	0%	0
Low risk Issues	25%	2
Informational Issues	50%	4

Summary of Findings

MetaScan security assessment was performed on **February 25, 2023 21:35:26** on project **KTX-core/** with the repository **https://github.com/KTX-finance/KTX-core/** on branch **default branch**. The assessment was carried out by scanning the project's codebase using the scan engine **Security Analyzer**. There are in total **8** vulnerabilities / security risks discovered during the scanning session, among which **2** critical vulnerabilities, **0** high risk vulnerabilities, **0** medium risk vulnerabilities, **2** low risk vulnerabilities, **4** informational issues.

ID	Description	Severity	Alleviation
MSA-001	Unuseable functions with no return value	Critical	Fixed
MSA-002	Wrong Target Address in the balanceOf Function	Critical	Fixed
MSA-003	Unused return value in contracts/tokens/YieldToken.sol.json	Low risk	Acknowledged
MSA-004	Unused return value in contracts/tokens/YieldToken.sol.json	Low risk	Acknowledged
MSA-005	Redundant payable keyword	Informational	Fixed
MSA-006	Lack of Check on the Arrays' Length	Informational	Acknowledged
MSA-007	Unused Imports	Informational	Fixed
MSA-008	Boolean equality in contracts/tokens/TokenVesting.sol	Informational	Fixed

2023-02-25

Findings

Critical (2)

1. Unuseable functions with no return value

Critical Security Analyzer

In function `balanceOf` and `totalSupply`, there is no return value in the function body, the return value `balanceOf` and `totalSupply` will return 0

File(s) Affected

contracts/staking/StakedKlp.sol #65-71

Examples

```
65      function balanceOf(address _account) external view returns (uint256) {
66          IRewardTracker(stakedKlpTracker).depositBalances(_account, klp);
67      }
...
69      function totalSupply() external view returns (uint256) {
70          IERC20(stakedKlpTracker).totalSupply();
71      }
```

Recommendation

Add return keyword with `return IRewardTracker(stakedKlpTracker).depositBalances(_account, klp);` and `return IERC20(stakedKlpTracker).totalSupply();`

Alleviation Fixed

-

2. Wrong Target Address in the balanceOf Function

Critical Security Analyzer

The target address in the balanceOf function is stakedKlpTracker. However, the target address of the balanceOf function in the GMX protocol is feeGlpTracker instead of stakedKlpTracker. `function balanceOf(address _account) external view returns (uint256) { return IRewardTracker(feeGlpTracker).depositBalances(_account, glp); }`

File(s) Affected

contracts/staking/StakedKlp.sol #65-68

Examples

```
65      function balanceOf(address _account) external view returns (uint256) {
66          IRewardTracker(stakedKlpTracker).depositBalances(_account, klp);
67      }
68
```

Recommendation

We advise correcting the target address of the `balanceOf` function.`

Alleviation Fixed

-

High risk (0)

No High risk vulnerabilities found here

Medium risk (0)

No Medium risk vulnerabilities found here

Low risk (2)

1. Unused return value in contracts/tokens/YieldToken.sol.json

Low risk Security Analyzer

Either the return value of an external call is not stored in a local or state variable, or the return value is declared but never used in the function body.

File(s) Affected

contracts/tokens/YieldToken.sol #101-106 #108-113

Examples

```
101     function recoverClaim(address _account, address _receiver) external onlyAdmin {
102         for (uint256 i = 0; i < yieldTrackers.length; i++) {
103             address yieldTracker = yieldTrackers[i];
104             IYieldTracker(yieldTracker).claim(_account, _receiver);
105         }
106     }
107
```

Recommendation

Ensure the return value of external function calls is used. Remove or comment out the unused return function parameters.

Alleviation Acknowledged

-

2. Unused return value in contracts/tokens/YieldToken.sol.json

Low risk Security Analyzer

Either the return value of an external call is not stored in a local or state variable, or the return value is declared but never used in the function body.

File(s) Affected

contracts/tokens/YieldToken.sol #101-106 #108-113

Examples

```
101     function recoverClaim(address _account, address _receiver) external onlyAdmin {
102         for (uint256 i = 0; i < yieldTrackers.length; i++) {
103             address yieldTracker = yieldTrackers[i];
104             IYieldTracker(yieldTracker).claim(_account, _receiver);
105         }
106     }
107
```

Recommendation

Ensure the return value of external function calls is used. Remove or comment out the unused return function parameters.

Alleviation Acknowledged

Informational (4)

1. Redundant payable keyword

Informational Security Analyzer

The token token is an ERC20 token. Its transfer does not require an address to be a payable address. Thus, there is no need to do the type conversion to make vestingSchedule.beneficiary a payable address.

File(s) Affected

contracts/tokens/TokenVesting.sol #228-246

Examples

```
238         uint256 vestedAmount = _computeReleasableAmount(vestingSchedule);
239         require(vestedAmount >= amount, "tv: no enough vested");
240         vestingSchedule.released = vestingSchedule.released.add(amount);
241         address payable beneficiaryPayable = payable(
242             vestingSchedule.beneficiary
243         );
244         vestingSchedulesTotalAmount = vestingSchedulesTotalAmount.sub(amount);
245         token.safeTransfer(beneficiaryPayable, amount);
246     }
247
248     /**
```

Recommendation

We advise removing the redundant type conversion.

Alleviation Fixed

-

2. Lack of Check on the Arrays' Length

Informational Security Analyzer

The token token is an ERC20 token. Its transfer does not require an address to be a payable address. Thus, there is no need to do the type conversion to make vestingSchedule.beneficiary a payable address.

File(s) Affected

contracts/peripherals/Timelock.sol #559-567
contracts/core/ShortsTracker.sol #92-99

Examples

```
559     function batchSetBonusRewards(
560         address _vester,
561         address[] memory _accounts,
  •••
565             _accounts.length == _amounts.length,
566             "Timelock: invalid lengths"
567         );
```

Recommendation

We advise removing the redundant type conversion.

Alleviation Acknowledged

-

3. Unused Imports

Informational Security Analyzer

The imported contract console.sol is unused in the protocol. Thus, it could be removed. The console.sol contract is used for debugging, and its usages in the TokenVesting contract are already marked as comments. Thus, it could be removed along with comments in the TokenVesting contract related to it.

File(s) Affected

contracts/tokens/TokenVesting.sol #1-10
contracts/core/VaultUtils.sol #1-10
contracts/core/Vault.sol #1-14

Examples

```
// contracts/TokenVesting.sol
// SPDX-License-Identifier: Apache-2.0
pragma experimental ABIEncoderV2;
...
import "../libraries/token/SafeERC20.sol";
import "../libraries/utils/ReentrancyGuard.sol";
import "../access/Governable.sol";
```

Recommendation

We advise removing the unused imported contract.

Alleviation Fixed

-

4. Boolean equality in contracts/tokens/TokenVesting.sol

Informational Security Analyzer

Boolean constants can be used directly and do not need to compare to true or false.

File(s) Affected

contracts/tokens/TokenVesting.sol #57-60 #65-69 #191-209 #326-372

Examples

```
     * @dev Reverts if no vesting schedule matches the passed identifier.
     */
    modifier onlyIfVestingScheduleExists(bytes32 vestingScheduleId) {
        require(vestingSchedules[vestingScheduleId].initialized == true);
        _;
    }
```

Recommendation

Just use boolean constants directly.

Alleviation Fixed

-

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.