



METATRUST

# Security Assessment for **XHash**

April 23, 2023






## Executive Summary

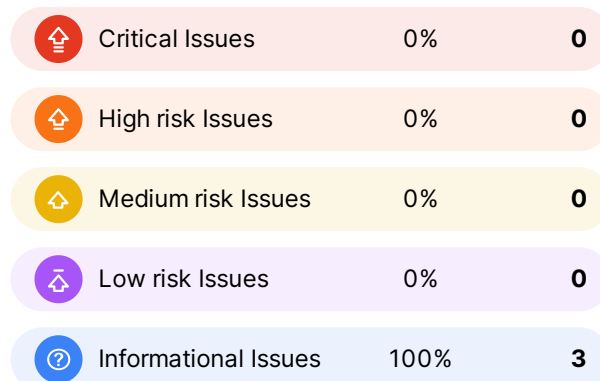
Overview		
Project Name	XHash	
Codebase URL	-	
Scan Engine	Security Analyzer	
Scan Time	2023/04/23 19:23:44	
Commit Id	-	

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

Critical Issues	 <p>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.</p>
High Risk Issues	 <p>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.</p>
Medium Risk Issues	 <p>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.</p>
Low Risk Issues	 <p>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.</p>
Informational Issue	 <p>The issue does not pose an immediate risk but is relevant to security best practices or Defence in Depth.</p>



## Summary of Findings

MetaScan security assessment was performed on **April 23, 2023 19:23:44** on project **XHash** with the repository **XHash** on branch **-**. The assessment was carried out by scanning the project's codebase using the scan engine **Security Analyzer**. There are in total **3** vulnerabilities / security risks discovered during the scanning session, among which **0** critical vulnerabilities, **0** high risk vulnerabilities, **0** medium risk vulnerabilities, **0** low risk vulnerabilities, **3** informational issues.

ID	Description	Severity	Alleviation
MSA-001	Unnecessary type conversion in the loop	Informational	Acknowledged
MSA-002	Centralized Risk	Informational	Acknowledged
MSA-003	Unnecessary usage of ReentrancyGuard	Informational	Acknowledged

## Findings

### Critical (0)

No Critical vulnerabilities found here

### High risk (0)

No High risk vulnerabilities found here

### Medium risk (0)


No Medium risk vulnerabilities found here


### Low risk (0)

No Low risk vulnerabilities found here

### Informational (3)

#### 1. Unnecessary type conversion in the loop

 Informational

 Security Analyzer

In the deposit function, within the loop, the depositContract address undergoes a type conversion to IDepositContract on every iteration. This repeated type conversion leads to unnecessary gas consumption. The exact gas savings depend on various factors such as the number of iterations in the loop and the current gas prices. However, a rough estimate is that a single type conversion costs around 10-20 gas units. By performing the conversion only once, rather than on each iteration, the gas savings would be approximately 10-20 gas units multiplied by (number of iterations - 1). For example, if there are 50 iterations, the gas savings would be around 490-980 gas units.

##### File(s) Affected

XHashEth2Depositor.sol #81-88

```
81
82 IDepositContract(address(depositContract)).deposit{value: collateral}(
83     pubkeys[i],
84     withdrawal_credentials[i],
85     signatures[i],
86     deposit_data_roots[i]
87 );
88
```



##### Recommendation

Move the type conversion outside the loop, perform it only once, and store the result in a local variable. By doing so, the gas cost associated with type conversion is reduced, as it will only be performed once, regardless of the number of iterations.

**Alleviation** Acknowledged

When the deposit method is called, 10-20 gas can be used in one cycle, which is very small, less than 1/3000.

## 2. Centralized Risk

 Informational Security Analyzer

The contract includes pause and unpause functions, which allow the contract owner to pause and unpause the contract's functionality. These functions are protected by the onlyOwner modifier, which restricts access to only the contract owner. While this provides the owner with control over the contract's operations, it also introduces a centralization risk, as the owner has the power to halt the contract's functionality at any time.

- The pause and unpause functions can be called only by the contract owner.
- The onlyOwner modifier is used to restrict access to these functions.
- The contract owner can unilaterally modify the paused state of the contract, potentially impacting users' ability to interact with the contract.

### File(s) Affected

XHashEth2Depositor.sol #101-114

```
101 function pause() public onlyOwner {
102     _pause();
103 }
104
105 /**
106  * @dev Returns to normal state.
107  *
108  * Requirements:
109  *
110  * - The contract must be paused.
111  */
112 function unpause() public onlyOwner {
113     _unpause();
114 }
```



### Recommendation

Consider implementing a decentralized governance mechanism or a multi-signature scheme that requires consensus among multiple parties before pausing or unpausing the contract. This can help mitigate the centralization risk associated with a single owner controlling critical contract functions. Alternatively, you can provide a clear justification for the centralization aspect and ensure that users are aware of the potential risks associated with a single point of control.

**Alleviation** Acknowledged

The contract is currently managed by XHash, and the management function is limited to the pause and unpause functions.

## 3. Unnecessary usage of ReentrancyGuard

 Informational Security Analyzer

The contract imports and inherits from the ReentrancyGuard contract, which is designed to protect against reentrancy attacks. However, the deposit function in this contract does not involve any interactions with external contracts, so the risk of reentrancy attacks is minimal. Including the ReentrancyGuard unnecessarily increases the contract's gas consumption and complexity.

### File(s) Affected

XHashEth2Depositor.sol #10-12

```
10
11 contract XHashEth2Depositor is ReentrancyGuard, Pausable, Ownable {
12
```

### Recommendation

Remove the ReentrancyGuard inheritance and import, as it is not required for the contract's functionality. This will reduce the contract's gas consumption and simplify the code, making it easier to read and maintain.

**Alleviation** Acknowledged

ReentrancyGuard is optional and does not affect security.

## 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.