



METATRUST

Pre Report for  
**ApusClub**

March 27, 2024

## Executive Summary

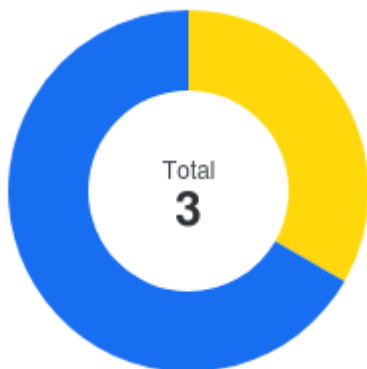
Overview			
Project Name	ApusClub		
Codebase URL	<a href="https://etherscan.io/token/0x594DaaD7D77592a2b97b725A7AD59D7E188b5bFa">https://etherscan.io/token/0x594DaaD7D77592a2b97b725A7AD59D7E188b5bFa</a>		
Scan Engine	Security Analyzer		
Scan Time	2024/03/27 08:00:00		
Commit Id	-		






  

Total			
Critical Issues	0		
High risk Issues	0		
Medium risk Issues	1		
Low risk Issues	0		
Informational Issues	2		

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	33%	1
	Low risk Issues	0%	0
	Informational Issues	67%	2

## Summary of Findings



MetaScan security assessment was performed on **March 27, 2024 08:00:00** on project **ApusClub** with the repository **eth/0x594DaaD7D77592a2b97b725A7AD59D7E188b5bFa** 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 **3** vulnerabilities / security risks discovered during the scanning session, among which **1** medium risk vulnerabilities, **2** informational issues.

ID	Description	Severity
MSA-001	Initial Token Allocation	Medium risk
MSA-002	Centralization Risk	Informational
MSA-003	Discussion: the social sites shown in the contract comment are invalid	Informational

## Findings

### Medium risk (1)

#### 1. Initial Token Allocation

 Medium risk Security Analyzer

When the contract deployed, all the tokens, 420,690,000,000 \$APU, are distributed to the deployer, which makes tokens over-centred to one person.

##### File(s) Affected

0x594DaaD7D77592a2b97b725A7AD59D7E188b5bFa.etherscan.io-ApusClubToken.sol #743-743



```
743         _mint(msg.sender, totalSupply);
```

##### Recommendation

Consider posting the detailed tokenomics of the \$APU and applying multi-sign tool to the centralized roles to mitigate the centralization risk.

### Informational (2)

#### 1. Centralization Risk

 Informational Security Analyzer

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

- `renounceOwnership`, leaves the contract without owner;
- `transferOwnership`, transfers ownership of the contract to a new account (`newOwner`).

##### File(s) Affected



0x594DaaD7D77592a2b97b725A7AD59D7E188b5bFa.etherscan.io-ApusClubToken.sol #1-1

```
1 // File: @openzeppelin/contracts/interfaces/draft-IERC6093.sol
```

##### 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.

#### 2. Discussion: the social sites shown in the contract comment are invalid

 Informational Security Analyzer

The social sites shown in the contract comments are below: **Website:** <http://apu.club/> **Twitter:** <https://twitter.com/apuclubeth>  
However, Both the website and the twitter are invalid.

We would like to inform client the misleading info in the contract comment.

**File(s) Affected**

0x594DaaD7D77592a2b97b725A7AD59D7E188b5bFa.etherscan.io-ApusClubToken.sol #731-736

```
731  /*
732  Find out more about Apu's Club:
733  Website: http://apu.club/
734  Twitter: https://twitter.com/apuclubeth
735
736  */
```

Audit Scope

File	SHA256	File Path
0×594DaaD7D77592a2b97b725A7AD59D7E188b5bFa.ethersc ApusClubToken.sol	547AD59D7E188b5bFa.ethersc 4867ac4a523f24f	/0×594DaaD7D77592a2b97b725A7AD59D7E188b5bFa.ethersc ApusClubToken.sol

## Disclaimer

This report is governed by the stipulations (including but not limited to service descriptions, confidentiality, disclaimers, and liability limitations) outlined in the Services Agreement, or as detailed in the scope of services and terms provided to you, the Customer or Company, within the context of the Agreement. The Company is permitted to use this report only as allowed under the terms of the Agreement. Without explicit written permission from MetaTrust, this report must not be shared, disclosed, referenced, or depended upon by any third parties, nor should copies be distributed to anyone other than the Company.

It is important to clarify that this report neither endorses nor disapproves any specific project or team. It should not be viewed as a reflection of the economic value or potential of any product or asset developed by teams or projects engaging MetaTrust for security evaluations. This report does not guarantee that the technology assessed is completely free of bugs, nor does it comment on the business practices, models, or legal compliance of the technology's creators.

This report is not intended to serve as investment advice or a tool for investment decisions related to any project. It represents a thorough assessment process aimed at enhancing code quality and mitigating risks inherent in cryptographic tokens and blockchain technology. Blockchain and cryptographic assets inherently carry ongoing risks. MetaTrust's role is to support companies and individuals in their security diligence and to reduce risks associated with the use of emerging and evolving technologies. However, MetaTrust does not guarantee the security or functionality of the technologies it evaluates.

MetaTrust's assessment services are contingent on various dependencies and are continuously evolving. Accessing or using these services, including reports and materials, is at your own risk, on an as-is and as-available basis. Cryptographic tokens are novel technologies with inherent technical risks and uncertainties. The assessment reports may contain inaccuracies, such as false positives or negatives, and unpredictable outcomes. The services may rely on multiple third-party layers.

All services, labels, assessment reports, work products, and other materials, or any results from their use, are provided "as is" and "as available," with all faults and defects, without any warranty. MetaTrust expressly disclaims all warranties, whether express, implied, statutory, or otherwise, including but not limited to warranties of merchantability, fitness for a particular purpose, title, non-infringement, and any warranties arising from course of dealing, usage, or trade practice. MetaTrust does not guarantee that the services, reports, or materials will meet specific requirements, be error-free, or be compatible with other software, systems, or services.

Neither MetaTrust nor its agents make any representations or warranties regarding the accuracy, reliability, or currency of any content provided through the services. MetaTrust is not liable for any content inaccuracies, personal injuries, property damages, or any loss resulting from the use of the services, reports, or materials.

Third-party materials are provided "as is," and any warranty concerning them is strictly between the Customer and the third-party owner or distributor. The services, reports, and materials are intended solely for the Customer and should not be relied upon by others or shared without MetaTrust's consent. No third party or representative thereof shall have any rights or claims against MetaTrust regarding these services, reports, or materials.

The provisions and warranties of MetaTrust in this agreement are exclusively for the Customer's benefit. No third party has any rights or claims against MetaTrust regarding these provisions or warranties. For clarity, the services, including any assessment reports or materials, should not be used as financial, tax, legal, regulatory, or other forms of advice.