METATRUST

Security Assessment for

Debox VI(2)

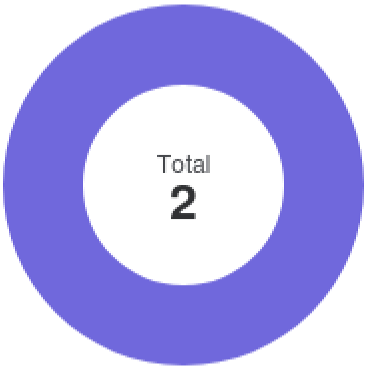
October 10, 2024

Executive Summary

Overview	
Project Name	Debox VI(2)
Codebase URL	https://github.com/debox-pro/debox_contracts
Scan Engine	Security Analyzer
Scan Time	2024/10/10 08:00:00
Commit Id	4074be51bbe9debf72e25515f123febf573e0d86

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.

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



Critical Issues	0%	0
High risk Issues	0%	0
Medium risk Issues	0%	0
Low risk Issues	100%	2
Informational Issues	0%	0

Summary of Findings

MetaScan security assessment was performed on **October 10, 2024 08:00:00** on project **Debox VI(2)** with the repository 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 **2** vulnerabilities / security risks discovered during the scanning session, among which **2** low risk vulnerabilities,

ID	Description	Severity	Alleviation
MSA-001	Initial Token Distribution	Low risk	Acknowledged
MSA-002	Lack of Invoking the `_disableInitializers` From The Constructor	Low risk	Fixed

Findings

Low risk (2)

1. Initial Token Distribution

Low risk Security Analyzer

In the contract DBXToken contract, during the deployment on Ethereum,

- 10,000,000 $BOX will be allocated to the wallet `0x2745F97f501087caF8eA740854Cfcac011fb34C3`,
- 20,000,000 $BOX will be allocated to the wallet `0x2745F97f501087caF8eA740854Cfcac011fb34C3`,
- 50,000,000 $BOX will be allocated to the wallet `0x5b1AfdB8C23569484773aF7bD4c98Af9ee7599D9`,
- 200,000,000 $BOX will be allocated to the wallet `0xa0c3d11eE7e5FFAF0f39b2f99dE7A7732f90a2aD`,
- 350,000,000 $BOX will be allocated to the wallet `0x37C8C7166B3ADCb1F58c1036d0272FbcD90D87Ea`,
- 200,000,000 $BOX will be allocated to the wallet `0xD0AE9A0b0596B9A68F56Ae629eaBfB8a58DA2F75`,
- 170,000,000 $BOX will be allocated to the wallet `0x866f585a1751D2A49aD67bf69Bce225F4e30dE8d`.

File(s) Affected

src/DeBoxToken.sol #22-29

```
22    constructor() ERC20Permit("DeBoxToken") ERC20("DeBoxToken", "BOX") {
23      _mint(0x2745F97f501087caF8eA740854Cfcac011fb34C3, 10_000_000 * 1e18);
24      _mint(0x2745F97f501087caF8eA740854Cfcac011fb34C3, 20_000_000 * 1e18);
25      _mint(0x5b1AfdB8C23569484773aF7bD4c98Af9ee7599D9, 50_000_000 * 1e18);
26      _mint(0xa0c3d11eE7e5FFAF0f39b2f99dE7A7732f90a2aD, 200_000_000 * 1e18);
27      _mint(0x37C8C7166B3ADCb1F58c1036d0272FbcD90D87Ea, 350_000_000 * 1e18);
28      _mint(0xD0AE9A0b0596B9A68F56Ae629eaBfB8a58DA2F75, 200_000_000 * 1e18);
29      _mint(0x866f585a1751D2A49aD67bf69Bce225F4e30dE8d, 170_000_000 * 1e18);
```

Recommendation

Consider posting the detailed tokenomics of the $BOX to mitigate the centralization risk of token distribution.

Alleviation Acknowledged

The team acknowledged this finding.

2. Lack of Invoking the `_disableInitializers` From The Constructor

Low risk Security Analyzer

In the commit `90c5b7f5e5663693a15bf6991e1e6f6fea5013e8`, the contract is updated to be upgradeable by inheriting contracts `UUPSUpgradeable`, and `OwnableUpgradeable`.

But, it lacks invoking the `_disableInitializers()` function from the constructor to avoid leaving a implementation contract uninitialized. An uninitialized contract can be taken over by an attacker. Reference: _disableInitializers | Openzepplin

File(s) Affected

Recommendation

Invoking the `_disableInitializers()` function from the constructor to avoid leaving a implementation contract uninitialized.

Alleviation Fixed

The team fixed this finding, in the commit 6ff5a8fa31cad291b69ffd3acf7971a0814686eb.

Audit Scope

File	SHA256	File Path
DeBoxTokenOFT.sol	b3f9342b9bdb1ec66d0437a2a58a401b2086f784e1f4bd7aa55ebd53b9e56eb8	/src/DeBoxTokenOFT.sol
DeBoxToken.sol	5d46d7b9ed535b66ec427600996233307649ec77302ff7116978efe43eb94f1c	/src/DeBoxToken.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.