Cyberscope

Audit Report

Seal

April 2024

Network	SOL
Type	SPL-Token
Address	3B3Zfs7eb46Re9GHWv6ccYRSBGy5EvQF2i2VXMD6tge6
Audited by	© cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit (Transfer Fee Authority)	Passed
●	MT	Mints Tokens (Mint Authority)	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses (Freeze Authority)	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
Medium	UA	Update Authority	Unresolved
Minor / Informative	ITA	Initial Token Allocation	Unresolved

Table of Contents

Review

Network	SOL
Explorer	https://solscan.io/token/3B3Zfs7eb46Re9GHWv6ccYRSBGy5EvQF2i2VXMD6tge6
Supply	1,000,000.00
Token Address	3B3Zfs7eb46Re9GHWv6ccYRSBGy5EvQF2i2VXMD6tge6
Token name	Seal (SEAL)
Owner Program	Token Program
Decimals	6
Metadata File Type	JSON
Badge Eligibility	Yes

Audit Updates

Initial Audit	12 Apr 2024

Overview

The `Seal` token symbolized as `SEAL`, is a distinguished SPL (Solana Program Library) token initialized using the `TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA` Token Program on the Solana blockchain, with a supply of `1,000,000` tokens. The token uses the URL https://nftstorage.link/ipfs/bafkreig3mtcgdeg4p36shc3zgc4kdkmoxsffg5w24tyiyyacd4sqcck25, which points to a decentralized storage service, while the image https://i.ibb.co/3r7bnBW/vhlvnb.jpg
is used for visual identification of the token across platforms and marketplaces. Overall, the Solana token is a distinct entity within the Solana network, identifiable by its unique characteristics as outlined in its metadata.

Metadata

The Metaplex Metadata provides details of the characteristics of the `Seal` token, a distinctive digital asset on the Solana blockchain tailored for utilizing the Metaplex Metadata. This metadata includes crucial information necessary for the asset's seamless integration and operation within the Solana ecosystem.

Specifically, the metadata was initiated by declaring the `8jdAy26dSB1LYrktfwmcNqhDyMWcJJqkoNv3hDuEJfrb` as the update authority attribute, which points to the account authorized to modify the metadata. The mint attribute specified the account `3B3Zfs7eb46Re9GHWv6ccYRSBGy5EvQF2i2VXMD6tge6` authorized for the initial token mint. The asset imposes `sellerFeeBasisPoints` of 0 basis points, indicating no transaction fee for trading is set. The metadata indicates that the asset has not yet undergone its primary sale as indicated by the `primarySaleHappened` value set to 0, and is marked as immutable since `isMutable` is 0, not allowing for future changes to the metadata. The `editionNonce` of 254 signifies a unique edition, while the `tokenStandard` of 2, aligns with a specified token standard within the Solana blockchain, ensuring its compatibility and standardization across the network. This detailed metadata structure offers a comprehensive overview of the token's key features and its operational framework within the Metaplex ecosystem on Solana.

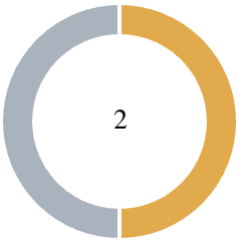

```
{
  "key": 4,
  "updateAuthority": "8jdAy26dSB1LYrktfwmcNqhDyMWcJJqkoNv3hDuEJfrb",
  "mint": "3B3Zfs7eb46Re9GHWv6ccYRSBGy5EvQF2i2VXMD6tge6",
  "data": {
    "name": "Seal",
    "symbol": "SEAL",
    "uri":
"https://nftstorage.link/ipfs/bafkreig3mtcgdeg4p36shc3zgc4kdkmoxsffg5w24tyiyya
cd4sqcck25a",
    "sellerFeeBasisPoints": 0,
    "creators": [
      {
        "address": "8jdAy26dSB1LYrktfwmcNqhDyMWcJJqkoNv3hDuEJfrb",
        "verified": 1,
```

```
        "share": 100
      }
    ]
  },
  "primarySaleHappened": 0,
  "isMutable": 1,
  "editionNonce": 253,
  "tokenStandard": 2,
  "collection": undefined,
  "uses": undefined,
}
```


Field	Value	Description
key	4	Account discriminator that identifies the type of metadata account
updateAuthority	8jdAy26dSB1LYrktfwmcNqhDyMWcJJqkoNv3hDuEJfrb	The public key that is allowed to update this account
mint	3B3Zfs7eb46Re9GHWv6ccYRSBGy5EvQF2i2VXMD6tge6	The public key of the Mint Account it derives from
name	Seal	The on-chain name of the token
symbol	SEAL	The on-chain symbol of the token
uri	https://nftstorage.link/ipfs/bafkreig3mtcgdeg4p36shc3zgc4kdkmoxsffg5w24tyiyyacd4sqcck25a	The URI to the external metadata. This URI points to an off-chain JSON file that contains additional data following a certain standard

sellerFeeBasisPoints	0	The royalties shared by the creators in basis points — This field is used by most NFT marketplaces, it is not enforced by the Token Metadata program itself
primarySaleHappened	0	A boolean indicating if the token has already been sold at least once. Once flipped to True, it cannot ever be False again. This field can affect the way royalties are distributed
isMutable	1	A boolean indicating if the metadata account can be updated. Once flipped to False, it cannot ever be True again
editionNonce	253	Unique identifier for this edition
tokenStandard	2	The standard of the token

Findings Breakdown



Critical	0
Medium	1
Minor / Informative	1

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	1	0	0	0
Minor / Informative	1	0	0	0

UA - Update Authority

Criticality	Medium
Status	Unresolved

Description

The contract is set up in a way that grants the update authority, with the address 8jdAy26dSB1LYrktfwmcNqhDyMWcJJqkoNv3hDuEJfrb, continued access to alter key metadata fields. This situation leaves the token exposed to potential hazards, as this address has the power to adjust critical attributes such as the token's name, symbol, and image. Without revoking these privileges from the update authority, there's a risk of unauthorized or harmful changes that could undermine the token's integrity and its intended use.

Recommendation

It is recommended to revoke the update authority privileges. This action would ensure a consistent security posture across the contract's operational aspects, eliminating the discrepancy that currently allows for undue modification privileges. Implementing this recommendation would align the contract's security measures, providing a more robust defense against unauthorized changes and enhancing the overall security of the contract's operational environment.

How to revoke the Update Authority:
https://www.quicknode.com/guides/solana-development/anchor/how-to-make-immutible-solana-programs#remove-the-update-authority-of-a-solana-program

ITA - Initial Token Allocation

Criticality	Minor / Informative
Status	Unresolved

Description

The token account `2sPoWrkgnq6qD4JXvaqYUqKYLRy54tXUMAS3MSXNGJZH`, holds a large portion of total supply. Consequently, at the time of the report, this address owns 78.51% of the entire token supply, amounting to 785,125 `KANE`. This concentration of almost the entire token supply in one address raises significant concerns about centralization within the token's ecosystem. Such a scenario creates a risk of market manipulation and could lead to other adverse effects, potentially undermining the token's decentralized nature and the overall health of its ecosystem.

Token Account	Quantity	Percentage
2sPoWrkgnq6qD4JXvaqYUqKYLRy54tXUMAS3MSXNGJZH	785,125	78.51%

Recommendation

It is recommended to distribute the tokens more broadly to achieve a more decentralized token holding structure. This can mitigate the risks associated with centralization and ensure a more stable and secure ecosystem for all participants. If the new address consists of a team's wallet address, then the team should carefully manage the private keys of that account. We strongly recommend implementing a robust security mechanism to prevent a single user from accessing the contract admin functions, such as a multi-sign wallet so that many addresses will confirm the action.

MT - Mint Tokens (Mint Authority)

Criticality	Passed
Status	Resolved

Description

The token has a fixed supply of tokens, as the mint authority has been revoked, ensuring a stable and unchangeable total supply. This key characteristic enhances its value proposition within the ecosystem by eliminating the possibility of future inflation of the token value through additional minting. This creates a predictable environment for investors and users, contributing to a perception of increased trustworthiness and security. This decision aligns with the best practices aiming to preserve the token's integrity and value, fostering a more sustainable and confident market presence.

The information regarding the revoke transaction of the mint authority can be accessed through the following link: https://solscan.io/tx/2Pb38zWfqimdzv6MLHhk4mW99avx75PhJ2ccZwmuwaLFtqcA3pLpSwmSpiCVm8KLJGSMRG7GpMnWJbYL8LE3diEz

Summary

The `Seal` token, built on the Solana network, leverages a solid architecture initiated via the Token program. This audit rigorously evaluates its performance, security, and compliance with best practices. The investigation aims to identify and address any operational vulnerabilities, performance bottlenecks, and areas for optimization, ensuring the token's robustness and reliability in the Solana ecosystem.

The token program analysis reported that the update authority privileges have not yet been revoked. This means that the token's metadata, including essential attributes like the token's name, symbol, description, and image, remains vulnerable to modification.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. 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 Cyberscope's prior written consent. 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 regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document 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 represents an extensive assessment 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 Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope'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 Cyberscope are subject to dependencies and are 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.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io