Cyberscope

Audit Report

SolSpend

March 2024

Network	SOL
Type	SPL-Token
Address	3mp1MN5v7zdGXTvvcC9zUMoszMrh9pNdaCDkAQKc7Fec
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	Unresolved
●	MT	Mints Tokens	Unresolved
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	UA	Update Authority	Unresolved

Table of Contents

Analysis **1**
Diagnostics **2**
Table of Contents **3**
Review **4**
Audit Updates 5
Source Files 5
Overview **6**
Transactions 7
Holders 8
Metadata 8
MetaplexMetadata 9
Metadata description 11
Findings Breakdown **14**
ELFM - Exceeds Fees Limit 15
Description 15
Recommendation 15
MT - Mints Tokens 16
Description 16
Recommendation 16
UA - Update Authority 17
Description 17
Recommendation 17
Summary **18**
Disclaimer **19**
About Cyberscope **20**

Review

Network	SOL
Explorer	https://solscan.io/token/3mp1MN5v7zdGXTvvcC9zUMoszMrh9pNdaCDkAQKc7Fec#txs
Current Supply	10,000,000.00
Website	www.SolSpend.io
Social Channels	https://twitter.com/SolSpend, https://t.me/SolSpend_Portal
Token name	SolSpend (SPEND)
Token address	3mp1MN5v7zdGXTvvcC9zUMoszMrh9pNdaCDkAQKc7Fec
Owner Program	Token Program
Authority	52K6QFiAqaz29nBLzWZtMt4UooAJFX7kMRitEbvfEUQx
Decimals	5
Signature	4gJiiPYiAhgcSeY4aWJe9dTdkapArt2587Xbyw6ZPkAkyAnoJa3S56s2urPKaBYKHf1WjNHRoKfxDC6L3tTrkxoN
Block	#255816885
Deploy Time	March 22, 2024 22:24:57 Eastern European Standard Time
Instructions	Compute-Budget-Set-Compute-Unit-Price, CreateAccount, Sol-Transfer, InitializeMint, CreateAssociatedAccount, MintTo, Create-Metadata-Account-V3
By	52K6QFiAqaz29nBLzWZtMt4UooAJFX7kMRitEbvfEUQx
MintTokens Authority	52K6QFiAqaz29nBLzWZtMt4UooAJFX7kMRitEbvfEUQx
FreezeAccount Authority	NONE

Metadata File Type	JSON
Name	SolSpend
Symbol	SPEND
Image	https://bafkreic4r56jg7fvkthkfzmmfy2z6ypfltqgowjvs44ghf32nh2nz77tva.ipfs.nftstorage.link
Total Transfers (At the time of the report)	0
Total Transactions (At the time of the report)	1
Total Holders (At the time of the report)	1

Audit Updates

Initial Audit	23 Mar 2024

Source Files

Filename	JSON
Metadata/JSON	https://solscan.io/token/3mp1MN5v7zdGXTvvcC9zUMoszMrh9pNdaCDkAQKc7Fec#metadata

Overview

The `SolSpend` token symbolized as `SPEND`, is a distinguished SPL (Solana Program Library) token initialized using the `TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA` Token Program on the Solana blockchain. The minting authority for the `SolSpend` token has not been renounced and is held by the entity, identified as `52K6QFiAqaz29nBLzWZtMt4UooAJFX7kMRitEbvfEUQx`. This allows for potential adjustments to the token's supply, offering a level of control over its distribution. The token uses the image URL https://bafkreic4r56jg7fvkthkfzmmfy2z6ypfltqgowjvs44ghf32nh2nz77tva.ipfs.nftstorage.link, which points to an image hosted on a decentralized storage service. This image is used for visual identification of the token across various platforms and marketplaces. Overall, the `SolSpend` token is a distinct entity within the Solana network, identifiable by its unique characteristics as outlined in its metadata.

Transactions

At the time of this report, the transactions of "SolSpend" token are as follows:

Signature	Block	Time (UTC)	Instructions	By	Fee (SOL)
4gJiiPYiAhgcSeY4aWJe9d...	#255816885	03-22-2024 20:24:57	Compute-Budget-Set-Compute-Unit-Price, CreateAccount, Sol-Transfer, InitializeMint, CreateAssociatedAccount, MintTo, Create-Metadata-Account-V3	52K6QF...vfEUQx	0.00013

Holders

At the time of this report, the holders of "SolSpend" token are as follows:

#	Token Account	Quantity	Percentage
1	G5xZsUGmcnpt8HyE8QGnvfVnhYXM2gibBmG5ZtdyRGAq	10,000,000	100.0000%

Metadata

MetaplexMetadata

The Metaplex Metadata provides details of the characteristics of the `SolSpend` token which uses the `SPEND` symbol, 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. The `updateAuthority` field is designated to the account capable of modifying this metadata, identified by the public key `52K6QFiAqaz29nBLzWZtMt4UooAJFX7kMRitEbvfEUQx`. Furthermore, the mint attribute specifies the account `3mp1MN5v7zdGXTvvcC9zUMoszMrh9pNdaCDkAQKc7Fec` authorized for the initial token mint.

```
{
  "key": 4,
  "updateAuthority": "52K6QFiAqaz29nBLzWZtMt4UooAJFX7kMRitEbvfEUQx",
  "mint": "3mp1MN5v7zdGXTvvcC9zUMoszMrh9pNdaCDkAQKc7Fec",
  "data": {
    "name": "SolSpend",
    "symbol": "SPEND",
    "uri":
"https://bafkreiee4afxw7jts4ccaqyk2g3exppkf5ru7u7hnusu7pq4qi62ataaze.ipfs.
nftstorage.link",
    "sellerFeeBasisPoints": 0
  },
  "primarySaleHappened": 0,
  "isMutable": 1,
  "editionNonce": 255,
  "tokenStandard": 2,
  "name": "SolSpend",
  "symbol": "SPEND",
  "image":
"https://bafkreic4r56jg7fvkthkfzmmfy2z6ypfltqgowjvs44ghf32nh2nz77tva.ipfs.
nftstorage.link",
  "description": "SolSpend is the first Non-KYC off ramp on Solana that
offers a wide variety of worldwide retailers via giftcards as well as
prepaid Mastercard and Visa cards. That allows users to pay direct with
Solana, while rewarding $SPEND Holders with the majority of the total
revenue generated. \n\nhttps://t.me/SolSpend_Portal \n\nwww.SolSpend.Io",
  "extensions": {
    "website": "www.SolSpend.io",
    "twitter": "https://twitter.com/SolSpend",
    "telegram": "https://t.me/SolSpend_Portal "
  },
  "tags": [],
  "creator": {
    "name": "SolSpend",
    "site": "https://www.solspend.io"
  }
}
```

Metadata description

The data section within the metadata discloses the asset's name as `SolSpend`, its trading symbol as `SPEND`, and the URI pointing to "https://bafkreiee4afxw7jts4ccaqyk2g3exppkf5ru7u7hnusu7pq4qi62ataaze.ipfs.nftstorage.link". The asset imposes a seller fee of 0 basis points, indicating no transaction fee for trading was set in the deploying phase. The metadata indicates that the asset has not yet undergone its primary sale (`primarySaleHappened` : 0) and is marked as mutable (`isMutable` : 1), allowing for future changes to the metadata. An `editionNonce` of 255 denotes a unique edition, and the asset conforms to a specific token standard within the Solana network (`tokenStandard` : 2), ensuring its compatibility and standardization across the platform. This detailed metadata structure offers a comprehensive overview of `SolSpend` key features and its operational framework within the Metaplex ecosystem on Solana.

Field	Value	Description
key	4	Account discriminator that identifies the type of metadata account
updateAuthority	52K6QFiAqaz29nBLzWZtMt4UooAJFX7kMRitEbvfEUQx	The public key that is allowed to update this account
mint	3mp1MN5v7zdGXTvvcC9zUMoszMrh9pNdaCDkAQKc7Fec	The public key of the Mint Account it derives from
name	SolSpend	The on-chain name of the token
symbol	SPEND	The on-chain symbol of the token
uri	https://bafkreiee4afxw7jts4ccaqyk2g3exppkf5ru7u7hnusu7pq4qi62ataaze.ipfs.nftstorage.link	The URI to the external metadata. This URI points to an off-chain JSON file that contains additional data following a certain standard

image	https://bafkreic4r56jg7fvkthkfzmmfy2z6ypfltqgowjvs44ghf32nh2nz77tva.ipfs.nftstorage.link	URL pointing to the asset's logo
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	255	Unique identifier for this edition
tokenStandard	2	The standard of the token
description	SolSpend is the first Non-KYC off ramp on Solana that offers a wide variety of worldwide retailers via giftcards as well as prepaid Mastercard and Visa cards. That allows users to pay direct with Solana, while rewarding $SPEND Holders with the majority of the total revenue generated. https://t.me/SolSpend_Portal www.SolSpend.Io	The description of the asset

website	www.SolSpend.io	The website of the asset
twitter	https://twitter.com/SolSpend	The twitter of the asset
telegram	https://t.me/SolSpend_Portal	The telegram of the asset

Findings Breakdown

Critical	3
Medium	0
Minor / Informative	0

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	3	0	0	0
Medium	0	0	0	0
Minor / Informative	0	0	0	0

ELFM - Exceeds Fees Limit

Criticality	Critical
Location	SolSpend
Status	Unresolved

Description

The current metadata configuration of the token has the `isMutable` field set to `1`, which allows for future changes to the metadata. This enables the update authority to modify the `setTaxFeePercent` field, thereby adjusting the fee structure as desired. Consequently, the update authority may take advantage of it by setting the `setTaxFeePercent` variable to a high percentage value.

Recommendation

It is recommended to revoke the update authority's privileges. This action will prevent any future modifications to the metadata, including updates on fees, thereby ensuring that the `setTaxFeePercent` variable cannot be set to a disproportionately high value. Revoking these privileges effectively disables the ability to change the fees. One method to accomplish this is by adhering to the instructions provided in the guide available at Remove the Update Authority of a Solana Program

MT - Mints Tokens

Criticality	Critical
Location	SolSpend
Status	Unresolved

Description

The token is currently configured in a manner that grants the min authority account, identified by the `52K6QFiAqaz29nBLzWZtMt4UooAJFX7kMRitEbvfEUQx` address, the exclusive capability to mint new tokens at will. This unrestricted minting authority poses a significant risk of token inflation for the `SolSpend` token. If the minting capability is exercised without stringent controls or limitations, it could lead to a scenario where the supply of `SolSpend` tokens is significantly increased in a short period. Such an action would dilute the value of existing tokens, potentially leading to a loss of trust among investors and users, and ultimately, a decrease in the token's market value. This highlights a critical vulnerability in the token's economic model, where the potential for unchecked token creation could result in highly inflated token supply, undermining the asset's stability and value proposition.

Recommendation

It is recommended to revoke the `mint authority` to mitigate the risk of unchecked token inflation. Implementing a fixed supply model could significantly enhance the token's economic security and investor confidence. By removing or significantly restricting the ability to mint new tokens, the `SolSpend` token can maintain a stable supply, preserving its value and ensuring a fair and predictable market for all stakeholders.

UA - Update Authority

Criticality	Critical
Location	SolSpend
Status	Unresolved

Description

The contract is currently configured in a manner that allows the update authority, identified by the address `52K6QFiAqaz29nBLzWZtMt4UooAJFX7kMRitEbvfEUQx`, to retain privileges that enable the modification of crucial metadata fields. The failure to revoke the `update authority` leaves the token vulnerable to potential risks, as the designated address retains the capability to make changes to the metadata. This oversight could lead to unauthorized or malicious modifications that might compromise the integrity and intended functionality of the token.

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.

Summary

The SolSpend token, built on the Solana network, implements a robust smart contract structure that was initialized using the Token program, with analysis revealing 3 critical issues.

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