Cyberscope

Audit Report

WojakWifHat

March 2024

Network	SOL
Type	SPL-Token
Address	D8uUR1okbXUmgsMvHLacP9DeVBaryeRCpsdYDQ9Uv62r
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	Passed
🔵	BT	Burns Tokens	Passed
🔵	BC	Blacklists Addresses	Passed

Diagnostics

● Critical   ● Medium   ● Minor / Informative

Severity	Code	Description	Status
●	UA	Update Authority	Unresolved

Table of Contents

Review

Network	SOL
Explorer	https://solscan.io/token/D8uUR1okbXUmgsMvHLacP9DeVBaryeRCpsdYDQ9Uv62r
Fixed Supply	1,000,000,000
Token name	WojakWifHat (WOJWIFHAT)
Token address	D8uUR1okbXUmgsMvHLacP9DeVBaryeRCpsdYDQ9Uv62r
Owner Program	Token Program
Decimals	9
Signature	3k7pw6YsDYdN13c5hDQTrnpkYFz9JzrfeZFd8XAaf7tBpjFdSvNUydNZKacsVrtErJMM2d7NAk5gTRAQZvu3UXfV
Block	255486462
Deploy Time	March 21, 2024 07:36:04 Eastern European Standard Time
Instructions	CreateAccount, InitializeMint, CreateAssociatedAccount, MintTo, Create, SetAuthority, Sol-Transfer
By	7gRwRzaBCJMCf4rTGcdr594MMETJhxnx7K2jf2V85EdM
MintTokens Authority	Revoked
FreezeAccount Authority	None
Metadata File Type	JSON
Name	WojakWifHat
Symbol	WOJWIFHAT

Image	https://photos.pinksale.finance/file/pinksale-logo-upload/17109 94116611-088a72c9b6cf4052d2613e345f3bd9f3.png
Website	https://wojakwifhat.club/
Social Channels	https://t.me/WojakWifHatCLUB
Total Transfers (At the time of the report)	1
Total Transactions (At the time of the report)	2
Total Holders (At the time of the report)	2

Audit Updates

Initial Audit	22 Mar 2024

Source Files

Filename	JSON
Metadata/JSON	https://solscan.io/token/D8uUR1okbXUmgsMvHLacP9DeVBary eRCpsdYDQ9Uv62r#metadata

Overview

The `WojakWifHat` token symbolized as `WOJWIFHAT` , is a distinguished SPL (Solana Program Library) token initialized using the `TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA` Token Program on the Solana blockchain. The `WojakWifHat` token has a fixed supply of `1,000,000,000` tokens since the mint has been disabled. This ensures a stable and unchangeable total supply, enhancing its value proposition within the ecosystem. The token uses the image URL https://photos.pinksale.finance/file/pinksale-logo-upload/1710994116611-088a72c9b6cf40 52d2613e345f3bd9f3.png , which points to an image hosted on Arweave, a decentralized storage service. This image is used for visual identification of the token across various platforms and marketplaces. Overall, the `WojakWifHat` token is a distinct entity within the Solana network, identifiable by its unique characteristics as outlined in its metadata.

Transfers

At the time of this report, the transfers of the WojakWifHat token are as follows:

Signature	Time (UTC)	Type	From	To	Amount
5zK4c3t7kBz BuXWRT5...	03-21-2024 05:55:41	Spl-Transfer	7gRwRz...V 85EdM	AcYbJE. ..tBPc2h	800,730,096.1

Transactions

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

Signature	Block	Time	Instructions	By	Fee (SOL)
5zK4c3t7kBzBu XWRT5iY8AViY...	#255489103	03-21-2024 05:55:41	Compute-Bud get-Set-Comp ute-Unit-Price (2+)	7gRwRz... V85EdM	0.000035
3k7pw6YsDYdN1 3c5hDQTrnpkY...	#255486462	03-21-2024 05:36:04	CreateAccount (6+)	7gRwRz... V85EdM	0.00001

Holders

At the time of this report, the distribution of WojakWifHat token holders is as follows:

#	Token Account	Account	Quantity	Percentage
1	EeqAWb...yGECFx	AcYbJE...tBPc2h	800,730,096.1	80.0730%
2	8miMot...jedNKR	7gRwRz...V85EdM	199,269,903.9	19.9269%

Metadata

MetaplexMetadata

The Metaplex Metadata provides details of the characteristics of the `WojakWifHat` token which uses the `WOJWIFHAT` 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 `7gRwRzaBCJMCf4rTGcdr594MMETJhxnx7K2jf2V85EdM`. Furthermore, the mint attribute specifies the account `D8uUR1okbXUmgsMvHLacP9DeVBaryeRCpsdYDQ9Uv62r` authorized for the initial token mint.

```
{
  "key": 4,
  "updateAuthority": "7gRwRzaBCJMCf4rTGcdr594MMETJhxnx7K2jf2V85EdM",
  "mint": "D8uUR1okbXUmgsMvHLacP9DeVBaryeRCpsdYDQ9Uv62r",
  "data": {
    "name": "WojakWifHat",
    "symbol": "WOJWIFHAT",
    "uri":
"https://nftstorage.link/ipfs/bafkreigk3uz34pnddodosb6z72pjcrokpqfj6vysyt
5yjh5n4hhln4tfci",
    "sellerFeeBasisPoints": 0,
    "creators": [
      {
        "address": "7gRwRzaBCJMCf4rTGcdr594MMETJhxnx7K2jf2V85EdM",
        "verified": 1,
        "share": 100
      }
    ]
  },
  "primarySaleHappened": 0,
  "isMutable": 1,
  "editionNonce": 254,
  "tokenStandard": 2,
  "name": "WojakWifHat",
  "symbol": "WOJWIFHAT",
  "description":
"▌▒▒▒▒     █████ █████ █████ █ \n ██████     █   █    █ █ \n ▒▒▒▒
██▌     ▒▒██ █ \n─█ ███ ██ █ \n─█ ▒▒ ▒ █ █
    █ \n─█ ██ █ ███ █ \n─█ ██ ▒ █ ▒ █ \n─
─█ ▒█ ██ ▒▒ ██",
  "image":
"https://photos.pinksale.finance/file/pinksale-logo-upload/1710994116611-
088a72c9b6cf4052d2613e345f3bd9f3.png",
  "creator": {
    "name": "PinkSale",
    "site": "https://pinksale.finance"
  },
  "extensions": {
    "telegram": "https://t.me/WojakWifHatCLUB",
    "website": "https://wojakwifhat.club/"
  }
}
```

Metadata description

The data section within the metadata discloses the asset's name as `WojakWifHat` , its trading symbol as `WOJWIFHAT` , and an image URI pointing to "https://photos.pinksale.finance/file/pinksale-logo-upload/1710994116611-088a72c9b6cf4 052d2613e345f3bd9f3.png ". Notably, 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 254 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 WojakWifHat 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	7gRwRzaBCJMCf4rTGcdr 594MMETJhxnx7K2jf2V85 EdM	The public key that is allowed to update this account
mint	D8uUR1okbXUmgsMvHLa cP9DeVBaryeRCpsdYDQ9 Uv62r	The public key of the Mint Account it derives from
Name	WojakWifHat	The on-chain name of the token
Symbol	WOJWIFHAT	The on-chain symbol of the token
Uri	https://nftstorage.link/ipfs/ bafkreigk3uz34pnddodosb 6z72pjcrokpqfj6vysyt5yjh5 n4hhln4tfci	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	254	Unique identifier for this edition
tokenStandard	2	The standard of the token
description	-	Description of the asset
image	https://photos.pinksale.finance/file/pinksale-logo-upload/1710994116611-088a72c9b6cf4052d2613e345f3bd9f3.png	URI pointing to the asset's logo.
Telegram	https://t.me/WojakWifHatCLUB	The telegram of the token.
Website	https://wojakwifhat.club/	The website of the token.

Findings Breakdown
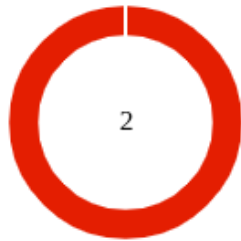
	Critical	2
	Medium	0
	Minor / Informative	0

Severity	Unresolved	Acknowledged	Resolved	Other
● Critical	2	0	0	0
● Medium	0	0	0	0
● Minor / Informative	0	0	0	0

ELFM - Exceeds Fees Limit

Criticality	Critical
Location	WojakWifHat
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

UA - Update Authority

Criticality	Critical
Location	WojakWifHat
Status	Unresolved

Description

The contract is set up in a way that grants the update authority, with the address `7gRwRzaBCJMCf4rTGcdr594MMETJhxnx7K2jf2V85EdM`, 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.

Summary

The WojakWifHat token, built on the Solana network, implements a robust smart contract structure that was initialized using the Token program, with analysis revealing 2 critical issues.

The contract's mint authority has been renounced. The information regarding the transaction can be accessed through the following link:

https://solscan.io/tx/3k7pw6YsDYdN13c5hDQTrnpkYFz9JzrfeZFd8XAaf7tBpjFdSvNUydNZKacsVrtErJMM2d7NAk5gTRAQZvu3UXfV.

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