Cyberscope

Audit Report

ORLY

November 2024

Network	SOL
Address	BNzPFfMKHX6REQGdLZhHC3qUEZmgkWQZ7dHTSygCttv6
Audited by	© cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	STMA	Mint Authority	Passed
●	STFA	Freeze Authority	Passed
●	STUA	Update Authority	Unresolved

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
Critical	Highly Likely / High Impact
Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
Minor / Informative	Unlikely / Low to no Impact

Review

Network	Solana
Address	BNzPFfMKHX6REQGdLZhHC3qUEZmgkWQZ7dHTSygCttv6
Explorer	https://solscan.io/address/BNzPFfMKHX6REQGdLZhHC3qUEZmgkWQZ7dHTSygCttv6
Name	ORLY
Symbol	ORLY
Decimals	6
Total Supply	1,000,000,000
Metadata File Type	JSON
Owner Program	https://solscan.io/address/TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA
Badge Eligibility	Yes

Audit Updates

Initial Audit	23 Nov 2024

Overview

The ORLY token symbolized as ORLY, is a distinguished SPL (Solana Program Library) token initialized using the `TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA` Token Program on the Solana blockchain, with a supply of 1,000,000,000 tokens. The token uses the URL https://cdn.pinksale.finance/file/pinksale-metadata/tokens/1732347251628-c6213a2c095ec129e137284226fffd88.json, which points to a decentralized storage service, while the image https://i.ibb.co/0FKQGYJ/IMG-20241123-082857-256-ezgif-com-resize-1.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.

Field	Value	Description
updateAuthority	FWWpNAyLBjfVALtN33hWAkLjpFHuWezPNkqfx3a6r5G8	The public key that is allowed to update this account
mint	BNzPFfMKHX6REQGdLZhHC3qUEZmgkWQZ7dHTSygCttv6	The public key of the Mint Account it derives from
name	O RLY?	The on-chain name of the token
symbol	ORLY	The on-chain symbol of the token
uri	https://cdn.pinksale.finance/file/pinksale-metadata/tokens/1732347251628-c6213a2c095ec129e137284226fffd88.json	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	false	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	true	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

Metadata

The Metaplex Metadata provides details of the characteristics of the `ORLY 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.

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 it is mutable since `isMutable` is true, allowing future changes to the metadata. The `editionNonce` of 253 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.


```
{
  "name": "O RLY?",
  "symbol": "ORLY",
  "description": "",
  "image":
"https://i.ibb.co/0FKQGYJ/IMG-20241123-082857-256-ezgif-com-resize-1.jp
g",
  "creator": {
    "name": "PinkSale",
    "site": "https://www.pinksale.finance"
  },
  "extensions": {}
}
```

Findings Breakdown

Critical	0
Medium	1
Minor / Informative	0

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

STMA - 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.

STFA - Freeze Authority

Criticality	Passed
Status	Resolved

Description

The freeze authority of the token has been revoked, permanently disabling the ability to freeze and thaw accounts. This action signals a definitive stance on account management within the token's ecosystem, emphasizing the permanence of account statuses. Removing the possibility of altering account states, establishes a more secure environment for token holders, reinforcing the network's commitment to stability and reliability. This decision reflects adherence to best security practices, aiming to solidify investor confidence and enhance the token's value by ensuring consistent operational integrity.

STUA - Update Authority

Criticality	Medium
Status	Unresolved

Description

The contract is set up in a way that grants the update authority, with the address `FWWpNAyLBjfVALtN33hWAkLjpFHuWezPNkqfx3a6r5G8` , 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

Summary

The ORLY 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 of the token has not yet been revoked. This situation leaves the token's operations regarding updating action, open to modifications. Consequently, this critical operation remains exposed to potential adjustments by the owner.

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

cyberscope.io