Cyberscope

Audit Report

XBUZZ

February 2025

Network	SOL
Address	Bg1MwHzZusomQqqFsGKkhjqj3tiefjXu4YFemPmWM4dg
Audited by	© cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	STMA	Mint Authority	Passed
●	STFA	Freeze Authority	Passed
●	ST2ETFC	Excessive Transfer Fee Configuration	Unresolved
●	ST2TMM	Token Modifiable Metadata	Unresolved

Table of Contents

Review

Network	Solana
Address	Bg1MwHzZusomQqqFsGKkhjqj3tiefjXu4YFemPmWM4dg
Explorer	https://solscan.io/address/Bg1MwHzZusomQqqFsGKkhjqj3tiefjXu4YFemPmWM4dg
Name	XBUZZ
Symbol	XBUZZ
Decimals	6
Total Supply	1,000,000,000,000
Metadata File Type	JSON
Owner Program	https://solscan.io/address/TokenzQdBNbLqP5VEhdkAS6EPFLC1PHnBqCXEpPxuEb
Badge Eligibility	Must Fix Criticals

Audit Updates

Initial Audit	19 Feb 2025

Overview

The xbuzz token symbolized as XBUZZ, is a distinguished SPL (Solana Program Library) token initialized using the `TokenzQdBNbLqP5VEhdkAS6EPFLC1PHnBqCXEpPxuEb` Token Program on the Solana blockchain, with a supply of 1,000,000,000,000 tokens. The token uses the URL https://ipfs.io/ipfs/bafkreifpavg24aeommmxzflvdze3gqkbwmu44xnulgai4jxyuntjh5vzoe, which points to a decentralized storage service, while the image 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
mint	Bg1MwHzZusomQqqFsGKkhjqj3tiefjXu4YFemPmWM4dg	The public key of the Mint Account it derives from
name	XBUZZ	The on-chain name of the token
symbol	XBUZZ	The on-chain symbol of the token
uri	https://ipfs.io/ipfs/bafkreifpavg24aeommmxzflvdze3gqkbwmu44xnulgai4jxyuntjh5vzoe	The URI to the external metadata. This URI points to an off-chain JSON file that contains additional data following a certain standard

Findings Breakdown

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	1	0	0	0
Medium	0	0	0	0
Minor / Informative	1	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The token has a fixed supply of tokens, as the mint authority has been revoked, ensuring a stable and unchangeable total supply.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.

ST2ETFC - Excessive Transfer Fee Configuration

Criticality	Critical
Status	Unresolved

Description

The token program has implemented the `transferFeeConfig` extension, which is currently configured to potentially allow fees that exceed the critical threshold of 2500 basis points, equivalent to 25% of the transaction value. This extension empowers the `transferFeeConfigAuthority` to enforce a protocol-level fee on every token transfer, where a portion of the tokens is withheld from the recipient and controlled by a designated authority. While this feature enhances the capability to monetize token transfers directly within the protocol, setting fees at such a high rate can severely impede token liquidity and may be viewed unfavorably by users and investors, diminishing the token's attractiveness and usability.

Recommendation

To address the issue of excessive fees configured through the transferFeeConfig extension, it is imperative to adjust the fee settings to ensure that they do not exceed a 25% limit. This alignment with reasonable market practices is essential for maintaining user trust and enhancing the token’s marketability. Ensuring that transaction costs do not become a burden will enhance user retention and support a healthy ecosystem. Furthermore, the team should carefully manage the private keys of the transferFeeConfigAuthority account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the extension’s functionalities.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Set the transferFeeBasisPoints less than 2500 and revoke the transferFeeConfigAuthority authority, which will eliminate the issues caused by the extension but it is non-reversible.

ST2TMM - Token Modifiable Metadata

Criticality	Minor / Informative
Status	Unresolved

Description

The token program is currently susceptible to risks associated with mutable metadata due to non-renounced authorities within the metadata extensions. This setup permits unauthorized or unintended modifications to the token’s metadata, potentially leading to inconsistencies and misinformation that could affect the token's integrity and reliability within the ecosystem.

The use of the `metadataPointer` extension with an active authority that has not been renounced, allows changes to the metadata's designated pointing location.

The activation of the `tokenMetadata` extension where the `updateAuthority` remains non-revoked, enabling updates to the content of the token’s metadata.

Those conditions can facilitate unwanted alterations that compromise the token’s consistent representation and trustworthiness.

Recommendation

To mitigate these risks and ensure the stability and integrity of the token’s metadata, it is advisable to secure the metadata by revoking the relevant authorities.

For the `metadataPointer` extension, revoke the `authority` of the metadataPointer to permanently lock the metadata's location and eliminate the possibility of redirection.

For the `tokenMetadata` extension, revoke the `updateAuthority` to prevent any further modifications to the metadata content.

By taking those steps, the token program can safeguard against unauthorized changes, maintaining a reliable and consistent metadata structure that enhances user trust and token utility.

Summary

The xbuzz 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.

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