Cyberscope

Audit Report

Viking DEX

June 2024

Network	Stacks
Identifier	SP31BV8VGBSGAR453P6PEQ9SB3AMYMZ1ATBPWDGKY.viking
Audited by	© cyberscope

Table of Contents

Review

Explorer	https://explorer.hiro.so/txid/SP31BV8VGBSGAR453P6PEQ9SB3AMYMZ1ATBPWDGKY.viking?chain=mainnet
Contract Identifier	SP31BV8VGBSGAR453P6PEQ9SB3AMYMZ1ATBPWDGKY.viking
Network	Stacks
Symbol	VIKI
Decimals	6
Total Supply	1,000,000,000

Audit Updates

Initial Audit	07 Jun 2024

Source Files

Filename	SHA256
odin-tkn.clar	10a3dc51d0281bea618c9b49f3e23c8bb843afa53b41ba1e2a8a8f65d4229bd6

Overview

The smart contract is an implementation of a fungible token on the Stacks blockchain, adhering to the SIP-010 standard. It defines a fungible token named "Viking" with the symbol "VIKI" and a precision of 6 decimal places. The contract includes standard functionalities for token transfer, balance inquiry, total supply check, and token burning. Specifically, it allows users to transfer tokens to other principals, including an optional memo for each transfer. The contract owner has the ability to set and update the token's metadata URI, which provides additional information about the token.

To facilitate these operations, the contract implements public functions such as transfer, get-name, get-symbol, get-decimals, get-balance, get-total-supply, set-token-uri, and burn. Additionally, it includes utility functions like send-many, which allows batch transfers to multiple recipients, and private helper functions check-err, send-token, and send-token-with-memo to manage internal logic. Upon deployment, the contract mints a predefined number of tokens to the contract owner. The design ensures that only authorized actions are performed by incorporating necessary checks and assertions, particularly around the ownership and authorization mechanisms.

Findings Breakdown

Critical	0
Medium	0
Minor / Informative	3

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

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	ITA	Initial Token Allocation	Unresolved
●	MMCR	Metadata Mutation Centralization Risk	Unresolved
●	NMA	Notification Mechanism Absence	Unresolved

ITA - Initial Token Allocation

Criticality	Minor / Informative
Location	viking.clar#L94
Status	Unresolved

Description

During the deployment of the contract, the account `SP31BV8VGBSGAR453P6PEQ9SB3AMYMZ1ATBPWDGKY` acquires the entire token supply of the token. This concentration of 100% of the token supply in some addresses 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.

```
(begin
  (try! (ft-mint? viking u1000000000000000 (var-get
contract-owner))
)
```

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 addresses consist of a team's wallet address, then the team should carefully manage the private keys of those accounts. 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.

MMCR - Metadata Mutation Centralization Risk

Criticality	Minor / Informative
Location	viking.clar#L49
Status	Unresolved

Description

The contract configuration grants the contract creator exclusive control over the token-uri variable. This allows for modifications to the URI that directs users to the token's metadata. The fact that the contract creator has the authority to modify the metadata URI, leaves the token vulnerable to potential risks, as the designated address retains the capability to make changes to the metadata. This could lead to unauthorized or malicious modifications that might compromise the integrity and intended functionality of the token.

```
(define-public (set-token-uri (value (string-utf8 256)))
    (if
        (is-eq tx-sender (var-get contract-owner))
            (ok (var-set token-uri (some value)))
        (err ERR-UNAUTHORIZED)
    )
)
```

Recommendation

To address this finding and mitigate centralization risks, it is recommended to evaluate the feasibility of migrating critical configurations and functionality into the contract's codebase itself. This approach would reduce external dependencies and enhance the contract's self-sufficiency. It is essential to carefully weigh the trade-offs between external configuration flexibility and the risks associated with centralization.

NMA - Notification Mechanism Absence

Criticality	Minor / Informative
Location	viking.clar#L49
Status	Unresolved

Description

The smart contract implementation allows the contract owner to update the `token-uri`, which contains metadata about the token. However, this implementation does not include a notification mechanism to inform users and external systems of such updates. The absence of a notification system means that any changes to the token metadata URI can occur without any alert or record, potentially leading to a lack of transparency and traceability. This could result in users and dependent systems being unaware of critical updates to the token metadata, which could affect the token's usability and trustworthiness.

```
(define-public (set-token-uri (value (string-utf8 256)))
    (if
        (is-eq tx-sender (var-get contract-owner))
            (ok (var-set token-uri (some value)))
        (err ERR-UNAUTHORIZED)
    )
)
```

Recommendation

To enhance transparency and ensure that all stakeholders are informed of changes to the token metadata, it is recommended to implement a notification mechanism within the `set-token-uri` function. This can be achieved by including a `print` statement that logs a notification whenever the `token-uri` is updated. The notification should contain relevant details such as the contract ID and the nature of the update. This will enable systems and users to be aware of and react to changes in the token metadata, thereby improving the overall robustness and trust in the contract.

Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
viking	Implementation			
	transfer	Public	✓	tx-sender
	get-name	Public		-
	get-symbol	Public		-
	get-decimals	Public		-
	get-balance	Public		-
	get-total-supply	Public		-
	set-token-uri	Public	✓	contract-owner
	get-token-uri	Public		-
	send-many	Public	✓	-
	check-err	Private	✓	-
	send-token	Private	✓	-
	send-token-with-memo	Private	✓	-
	burn	Public	✓	tx-sender

Summary

Viking DEX implements a token mechanism on the Stacks Blockchain. This audit investigates security issues, business logic concerns and potential improvements.

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