⚠ **Disclaimer** Not a financial advice.Always DYOR.

Latest Audit - 2024/02/25

Starck

0xA35b5C783117e107644056F5D39fAa468e9d8D47

Static analysis Dynamic analysis Symbolic Execution SWC check

STARCK is an AI token deployed on the Binance Smart Chain which monitors and analyzes Equity Markets, Commodity markets, Forex, Cryptocurrencies. Starck's team is developing AI Starck Investment Platform to monitor, analyze and send news about upcoming ups or downs in the trends of selected assets such as: commodities, quity, forex and cryptocurrencies. AI Starck Investment Platform is an innovative and powerful tool that is developed to help traders and investors get instant prices, news, analysis and tracking of a complete investment portfolio.

CONTRACT ADDRESS	NETWORK	LICENSE	COMPILER
0xA35b...9d8D47	Binance Smart Chain	MIT	v0.8.22

TYPE	LANGUAGE	REQUEST DATE	REVISION DATE
N/A	Solidity	2024/02/25	2024/02/25

CRITICAL	HIGH	MEDIUM
Passed	Passed	1 Issue

LOW	INFORMATIONAL	OPTIMIZATION
1 Issue	1 Issue	1 Issue

Owner privileges

Crucial issues found

The contract does contain issues of high or medium criticality. In some circumstances, the Contract may not function as intended and may pose a safety risk.

Contract owner cannot mint
It is not possible to mint new tokens.

Contract owner cannot blacklist addresses.
It is not possible to lock user funds by blacklisting addresses.

Contract owner cannot set high fees
The fees, if applicable, can be a maximum of 25% or lower. The contract can therefore not be locked. Please take a look in the comment section for more details.

Token transfer can be locked
Owner can lock user funds with owner functions.

Token cannot be burned
There is no burn function within the contract.

Ownership is not renounced
Contract can be manipulated by owner functions.

Comments

Ownership Privileges

- The owner can pause/un-pause token transfer for an indefinite period of time.

Note - This Audit report consists of a security analysis of the **Starck** smart contract. This analysis did not include functional testing (or unit testing) of the contract's logic. Moreover, we only audited one token contract for the **Starck** team. Other contracts associated with the project were not audited by our team. We recommend investors do their own research before investing.

Audit Scope

This audit covered the following files listed below with a SHA-1 Hash. The above token Team provided us with the files that needs to be tested.

We will verify the following claims:

- Correct implementation of Token standard
- Deployer cannot mint any new tokens
- Deployer cannot burn or lock user funds
- Deployer cannot pause the contract
- Overall checkup (Smart Contract Security)

The auditing process follows a routine series of steps:

- Review of the specifications, sources, and instructions provided to SolidProof to make sure we understand the size, scope, and functionality of the smart contract.
- Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to SolidProof describe.
- Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
- Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
- Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
- Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts.

A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

STARCK.sol
`f07e682be8291c6eda5e14449ed7126ca766cea6`

Audit Details

Throughout the review process, care was taken to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as there were discovered.

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Medium Issues

#1 ISSUE ⓘ

Pending

The owner lock tokens.

STARCK.SOL

L937-939

DESCRIPTION

The contract contains the pausable functionality, which can lock the token transfer for an indefinite period, which is not recommended as there must be a locking period in the contract so that the token transfer is not locked. Add a locking period in the contract so that the tokens are not locked for an indefinite period of time.

Low Issues

#1 ISSUE ⓘ

Pending

Floating pragma solidity version.

STARCK.SOL

L6

DESCRIPTION

Adding the constant version of solidity is recommended, as this prevents the unintentional deployment of a contract with an outdated compiler that contains unresolved bugs.

Informational Issues

#1 ISSUE ⓘ

Pending

Functions that are not used (dead-code)

STARCK.SOL

L188-190

DESCRIPTION

Remove unused functions.

Optimization Issues

#1 ISSUE ⓘ

Pending

Public function that could be declared external (external-function)

STARCK.SOL

L269-271 **L277-282** **L584-586** **L592-594** **L616-618** **L623-625**

L635-639 **L658-662** **L680-685** **L899-901** **L914-917** **L937-939**

L941-943

DESCRIPTION

Use the `external` attribute for functions never called from the contract.

Disclaimer

SSL Secured

SOLIDProof

MAKE Solutions UG
(haftungsbeschränkt)
Werkstrasse 10a
24983 Handewitt
Deutschland

E-Mail: hello@solidproof.io

Legal Notice
Privacy
GitHub
Medium
Unicrypt Network
Pathfund
Etherlite
CryptoAdventure