verichains

SECURITY AUDIT OF

VAPOR DAO

Public Report

Feb 07, 2024

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Sui Blockchain	Sui is an innovative, decentralized Layer 1 blockchain that redefines asset ownership. Sui Move feels like a paradigm change in web3 development. Treating objects as 1st class citizens brings composability to a whole new level. Polymedia. We are thrilled to be building on Sui.
Sui Object	The basic unit of storage in Sui is object. In contrast to many other blockchains where storage is centered around accounts and each account contains a key-value store, Sui's storage is centered around objects.
Move	Move is a new programming language that implements all the transactions on the Aptos/Sui blockchain.
Move Module	A Move module defines the rules for updating the global state of the Aptos/Sui blockchain. In the Aptos/Sui protocol, a Move module is a smart contract.
DAO	A digital Decentralized Autonomous Organization and a form of investor-directed venture capital fund.

EXECUTIVE SUMMARY

This Security Audit Report was prepared by Verichains Lab on Feb 07, 2024. We would like to thank the Vapor for trusting Verichains Lab in auditing smart contracts. Delivering high-quality audits is always our top priority.

This audit focused on identifying security flaws in code and the design of the Vapor DAO. The scope of the audit is limited to the source code files provided to Verichains. Verichains Lab completed the assessment using manual, static, and dynamic analysis techniques.

During the audit process, the audit team had identified no vulnerable issue in the smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About Vapor DAO

Vapor is a premier reserve currency ecosystem built on Sui, using Sui Move.Vapor is created to facilitate a new aspect to Sui Defi with a community-first mindset, and to elevate the overall Sui DeFi experience for users by offering a variety of Defi products (VAPOREON, inscriptions).Simply put, Vapor DAO an experimental Defi project on the Sui blockchain. The VAPOR currency is backed by a token treasury that is managed by the DAO. The DAO buys assets from investors (to be deposited in the Treasury) and issues VAPOR tokens to replace them.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the Vapor DAO. It was conducted on commit `3b9b9499be90d66a3a2747aa5cab52552e1e502b` from git repository *https://github.com/VaporDAO/sui-contracts*.

SHA256 Sum	File
`2059f7cf9b3e3d52c3bfd14bd32e3f68f5b318a3c0934f7fbf94d48f62e104a3`	`admin.move`
`d3540a828dd02c32c7a786864e1b8e5255ce48f9aa7b4b9bb2fa7e0d24d839ff`	`bond.move`
`c536ce301dcd2ddefc38bac27ca837e4c3080dbf0091d2922c2a346682255161`	`oracle.move`
`fe7ea1c558515be239695d299ca306a501003c752ea75e807081a887d1592dbc`	`stake.move`
`20d26c933d411df27bc56f21ac962cbf3287c3ee71dd96146b26b0e124e53dec`	`token.move`
`e75e52812259acc3c58029c322965dbe5a0dc38c61efcd4c7b9003b6c3dad330`	`vesting.move`

1.3. Audit methodology

Our security audit process for smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using public and RK87, our in-house smart contract security analysis tool.
- Manual audit of the codes for security issues. The contracts are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that were considered during the audit of the smart contract:

- Numerical precision errors
- Transaction-Ordering Dependence
- DoS with (Unexpected) revert
- Gas Usage, Gas Limit and Loops
- Logic Flaws

For vulnerabilities, we categorize the findings into categories as listed in table below, depending on their severity level:

SEVERITY LEVEL	DESCRIPTION
CRITICAL	A vulnerability that can disrupt the contract functioning; creates a critical risk to the contract; required to be fixed immediately.
HIGH	A vulnerability that could affect the desired outcome of executing the contract with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the contract with medium impact in a specific scenario; needs to be fixed.
LOW	An issue that does not have a significant impact, can be considered as less important.

Table 1. Severity levels

1.4. Disclaimer

Vapor acknowledges that the security services provided by Verichains, are conducted to the best of their professional abilities but cannot guarantee 100% coverage of all security vulnerabilities. Vapor understands and accepts that despite rigorous auditing, certain vulnerabilities may remain undetected. Therefore, Vapor agrees that Verichains shall not be held responsible or liable, and shall not be charged for any hacking incidents that occur due to security vulnerabilities not identified during the audit process.

1.5. Acceptance Minute

This final report served by Verichains to the Vapor will be considered an Acceptance Minute. Within 7 days, if no any further responses or reports is received from the Vapor, the final report will be considered fully accepted by the Vapor without the signature.

2. AUDIT RESULT

2.1. Overview

The Vapor DAO was developed using the Move programming language and deployed on the Sui Blockchain.

The Vapor DAO centralizes all privileged roles in the `admin` module. Each module has its owner and operator roles.

- `OwnerCap`: The owner of the module. This role is responsible for creating operators capabilities.
- `OperatorCap`: The operator of the module. This role is allowed to perform all operations on the module.

2.1.1. Bond Module

The smart contract manage a bonding system where users lock up tokens to receive vested `VAPOR` tokens, with an operator controlling parameters such as treasury, vesting duration, and bonded asset details.

2.1.2. Stake Module

Users can stake/unstake their `VAPOR` tokens, receiving a corresponding amount of staked tokens (`sVAPOR`) with `1:1` ratio.

2.1.3. Oracle Module

The smart contract is designed to manage and provide price information within the Vapor DAO ecosystem. It includes an administrative system where an admin can set the price for an asset, and users can query this price.

2.1.4. Vesting Module

The module allow user to vest a specified amount of tokens (via **Bond module**) over a defined duration and allows users to claim vested tokens based on the elapsed time.

2.1.5. Token Module

PROPERTY	VALUE
Name	Vapor DAO
Symbol	VAPOR
Decimals	6
Initial Supply	50,000 x10^6 (50 thousand)

Table 2. The VAPOR token contract properties

For token on SUI, the security audit team has the list of centralization issues below:

Checklist	Status
Upgradeable	Yes
Fee modifiable	No
Mintable	Yes

Table 3. The centralization checklist

2.2. Findings

During the audit process, the audit team found no vulnerability issue in the given version of Vapor DAO.

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Feb 07, 2024*	Public Report	Verichains Lab

Table 4. Report versions history