sevenhash

Security Audit

Disclaimer

Security audits cannot uncover all existing vulnerabilities; even an audit in which no vulnerabilities are found is not a guarantee of a secure system. However, code assessments enable the discovery of vulnerabilities that were overlooked during development and areas where additional security measures are necessary. In most cases, applications are either fully protected against a certain type of attack, or they are completely unprotected against it.

Some of the issues may affect the entire application, while some lack protection only in certain areas. This is why we carry out a source code audits aimed at determining all locations that need to be fixed. Within the customer-determined time frame, we performed an audit in order to discover as many vulnerabilities as possible.

The focus of our audit was limited to the code parts defined in the engagement letter. We assessed whether the project follows the provided specifications. These assessments are based on the provided threat model and trust assumptions. We draw attention to the fact that due to inherent limitations in any software development process and software product, an inherent risk exists that even major failures or malfunctions can remain undetected. Further uncertainties exist in any software product or application used during the development, which itself cannot be free from any error or failures.

These preconditions can have an impact on the system's code and/or functions and/or operation. We did not assess the underlying third-party infrastructure which adds further inherent risks as we rely on the correct execution of the included third-party technology stack itself.

Report readers should also take into account that over the life cycle of any software, changes to the product itself or to the environment in which it is operated can have an impact leading to operational behaviors other than those initially determined in the business specification.

Terminology & Risk Classification

For the purpose of this audit, we adopt the following terminology: To classify the severity of our findings, we determine the likelihood and impact (according to the CVSS risk rating methodology).

Likelihood: The likelihood of a finding to be triggered or exploited in practice.
Impact: The technical and business-related consequences of a finding.
Severity: An additive consideration based on the Likelihood and the Impact (as referenced below).

We use the table below to determine the severity of any and all findings. Please note that none of these risk classifications constitute endorsement or opposition to a particular project or contract.

		Impact	
Likelihood	High	Medium	Low
High	Severity: Critical	Severity: High	Severity: Medium
Medium	Severity: High	Severity: Medium	Severity: Low
Low	Severity: Medium	Severity: Low	Severity: Low

Summary

Contracts In-scope:
Token.sol

EtherScan:
https://etherscan.io/token/0x2e0a227ef31ecd32a37273d67212fa9185309fab#code

In the period 5 May. 2024 - 7 May. 2024 we audited REV3AL smart contract.

In this period of time a total of 0 of issues were found.

Severity	Issues
Critical Risk	0
High Risk	0
Medium Risk	0
Low Risk	0
Gas Optimization	0
Informational	0

Issues

Rev3al's smart contract is a standard ERC20 contract, leveraging the OpenZeppelin v5.0 libraries/mock-up contracts. The most recent audit conducted on the contract found no issues related to its ERC20 functionality, as detailed in OpenZeppelin's audit report from October 2023, which you can review here: https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/audits/2023-10-v5.0.pdf