PROTOFIRE

January 2026

Smart contract audit
rain.math.fixedpoint

Content

Project description **3**
Executive summary **3**
Reviews **3**
Technical analysis and findings **5**
Security findings **6**
**** Critical 6
*** High 6
** Medium 6
* Low 6
Informational 6
General Risks **7**
Approach and methodology **8**

Project description

This repository contains a Solidity library for 18 decimal fixed point math. It provides functionality for rescaling non-18 decimal fixed point values (e.g., ERC20 token amounts) to and from 18 decimals, enabling consistent arithmetic operations. It handles explicit rounding directions, works with simple uint256 values, and is designed to be a minimal, zero-dependency foundation compatible with libraries like OpenZeppelin.

Executive summary

Type	Library
Languages	Solidity
Methods	Architecture Review, Manual Review, Unit Testing, Functional Testing, Automated Review
Documentation	README.md
Repositories	https://github.com/rainlanguage/rain.math.fixedpoint

Reviews

Date	Repository	Commit
13/01/26	rain.math.fixedpoint	1752e9fbd635901ac7eb177699681ed97290e12e
26/01/26	rain.math.fixedpoint	1a0525ff62e6a25669dc62812bb6a755fbbeb414

Scope

Contracts
src/lib/LibFixedPointDecimalStrings.sol
src/lib/parse/LibFixedPointDecimalParse.sol
src/lib/LibFixedPointDecimalScale.sol
src/lib/LibFixedPointDecimalArithmeticOpenZeppelin.sol
src/lib/LibWillOverflow.sol

src/lib/format/LibFixedPointDecimalFormat.sol
src/lib/FixedPointDecimalConstants.sol
src/error/ErrParse.sol
src/error/ErrScale.sol

Technical analysis and findings

Critical	0
High	0
Medium	0
Low	0
Informational	0

Security findings

**** Critical

No critical severity issue found.

*** High

No high severity issue found.

** Medium

No Medium severity issue found.

* Low

No Low severity issue found.

Informational

No Informational severity issue found.

General Risks

- Precision Loss on Downscaling: Scaling down any fixed-point decimal reduces precision. This can lead to "dust" or, in worst-case scenarios, trapped funds if subsequent operations assume full precision. Users must strictly adhere to using the correct rounding flags (round up vs. round down) provided by the library to mitigate this, especially when handling user assets.

- Overflow with Extreme Values: While unlikely in typical token contexts (where values are ~1e40), the library relies on standard overflow behavior for values exceeding approximately 1e77 (standard uint256 limit when scaled). Use cases involving extremely large numbers or high-precision decimals must treat these edge cases with caution.

Approach and methodology

To establish a uniform evaluation, we define the following terminology in accordance with the OWASP Risk Rating
Methodology:

Likelihood
Indicates the probability of a specific vulnerability being discovered and exploited in real-world
scenarios

Impact
Measures the technical loss and business repercussions resulting from a successful attack

Severity
Reflects the comprehensive magnitude of the risk, combining both the probability of occurrence
(likelihood) and the extent of potential consequences (impact)

Likelihood and impact are divided into three levels: High H, Medium M, and Low L. The severity of a risk is a blend of these two factors, leading to its classification into one of four tiers: Critical, High, Medium, or Low.

When we identify an issue, our approach may include deploying contracts on our private testnet for validation through testing. Where necessary, we might also create a Proof of Concept PoC to demonstrate potential exploitability. In particular, we perform the audit according to the following procedure:

Advanced DeFi Scrutiny
We further review business logics, examine system operations, and place DeFi-related aspects
under scrutiny to uncover possible pitfalls and/or bugs

Semantic Consistency Checks
We then manually check the logic of implemented smart contracts and compare with the
description in the white paper.

Security Analysis
The process begins with a comprehensive examination of the system to gain a deep
understanding of its internal mechanisms, identifying any irregularities and potential weak spots.