PROTOFIRE

February 2026

Smart contract audit
rain.factory

Content

Project description

The rain.factory repository implements a generic, permissionless factory system for deploying EIP-1167 minimal proxies.

The core contract, CloneFactory, serves as a universal deployer that allows any implementation contract adhering to the ICloneableV2 interface to be cloned. Unlike legacy factory patterns that require unique factory contracts for each implementation type, rain.factory decouples the deployer from the logic, enabling a single factory to service an entire ecosystem of upgradeable or immutable patterns.

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.factory

Reviews

Date	**Repository**	**Commit**
11/02/26	rain.factory	1a92a8688249aa5a8f4e82d5ed584604515f1ea0

Scope

Contracts
src/concrete/CloneFactory.sol
src/interface/deprecated/ICloneableFactoryV1.sol
src/interface/deprecated/ICloneableV1.sol
src/interface/deprecated/IFactory.sol

src/interface/ICloneableFactoryV2.sol
src/interface/ICloneableV2.sol
src/lib/LibCloneFactoryDeploy.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.

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.