Safe Edges Security Assessment Report

Fluid Protocol

Assessment Date: October 20, 2024
Protocol: Fluid Protocol A decentralized liquidity platform for collateralized borrowing

---

Executive Summary

The Safe Edges team conducted a comprehensive security audit of the Fluid Protocol and identified **Multiple issues**. These findings were spread across core components including reward distribution, liquidation logic, oracle integration, and collateral management.

Summary of Findings:

- 2 Critical Issues Urgent security concerns with direct impact on funds or protocol stability
- 3 High Severity Issues High risk vulnerabilities with potential for fund loss or misbehavior
- 4 Medium Severity Issues Functional bugs affecting operational reliability
- 5 Low Severity Issues Minor vulnerabilities or edge-case risks
- 7 Informational Issues Recommendations for best practices and improvements

---

Critical Vulnerabilities

1. Reward Snapshot Misalignment

Severity: Critical
Status: Resolved

- **Description:** Partial liquidations did not update the borrower’s reward snapshot correctly.
- **Impact:** This led to reward miscalculations and the possibility of double-counted rewards.
- **Resolution:** Snapshots are now updated immediately post-liquidation; batch logic improved.

2. State Update Failure on Redemption Cancellation

Severity: Critical
Status: Resolved

- **Description:** Cancelling partial redemptions didn’t update trove state or reintegrate them into the sorted structure.
- **Impact:** Caused inconsistencies in system state.
- **Resolution:** Proper reinsertion and state syncing logic implemented.

High Severity Vulnerabilities

3. Incorrect Oracle Price Structure

Severity: High
Status: Resolved

- **Issue:** The oracle integration missed critical fields like confidence intervals and exponents.
- **Impact:** Risk of inaccurate price feeds affecting operations.
- **Resolution:** Updated to use full Pyth structure with validations.

4. Incorrect Trove Retrieval Logic

Severity: High
Status: Resolved

- **Issue:** Troves with the highest collateral ratio were used instead of the lowest.
- **Impact:** Allowed undercollateralized troves to persist.
- **Resolution:** Retrieval logic corrected to identify lowest-ratio positions first.

5. Timestamp Synchronization Flaw

Severity: High
Status: Resolved

- **Issue:** Time drift between on-chain timestamp and oracle could cause false reverts.
- **Impact:** Oracle data was rejected despite being valid.
- **Resolution:** Enhanced staleness logic to account for drift.

Medium Severity Issues

6. Trove Redemption Order Violation

Severity: Medium
Status: Resolved

- Reward calculations during redemption altered trove order unexpectedly.

7. Missing Validation Checks

Severity: Medium
Status: Resolved

- Batch liquidation lacked validations for sorting and duplication.

8. Imprecise Reward Distribution

Severity: Medium
Status: Resolved

- Pending rewards were excluded from stake-based reward calculation.

9. Validation Logic Inconsistency

Severity: Medium
Status: Resolved

- Insert position logic referenced incorrect node pointers.

Security Recommendations

Oracle Integration

- Validate oracle confidence intervals before using price data
- Account for time drift between off-chain and on-chain timestamps
- Follow oracle safety best practices

Liquidation System

- Validate trove states before processing
- Enforce risk-based ordering in liquidation logic
- Add edge-case checks to batch functions

Reward Mechanism

- Always update snapshots after state changes
- Reflect pending rewards in calculations
- Avoid state mismatches during batched logic

Code Quality

- Remove unnecessary checks
- Add zero-amount transfer validations
- Standardize access control and ownership patterns

Low Priority Improvements

Code Optimization

- Eliminate redundant logic and dead code
- Improve gas efficiency
- Enhance readability and modularity

Input Validation

- Validate all external input parameters
- Check asset IDs and token references properly
- Add detailed error messages for failed conditions

Time-based Operations

- Use precise time constants
- Optimize oracle timeouts

- Handle outdated prices more gracefully

Conclusion

The Fluid Protocol has addressed all critical and high-severity vulnerabilities discovered during the audit. Improvements were implemented across multiple layers including redemption logic, oracle integrations, liquidation handling, and reward mechanisms. These changes enhance the system's resilience, accuracy, and operational integrity.

While a few medium and low-priority issues remain as potential optimization areas, none pose direct threats to protocol safety. The Fluid Protocol is now well-prepared to operate securely under normal and edge-case conditions.

This report summarizes the findings of the security audit conducted by safeedges.in . All major concerns have been addressed to ensure the robustness and safety of the protocol's smart contracts.