# BUG REPORT

*Overflow bug in QUBIC smart contracts*

**Mundus**

13 Sep 2025

# Bug Report: QVE-2025-0001

| | |
|---|---|
| Bug ID | ***QVE-2025-0001*** |
| Finder | *Mundus team* |
| Date (reported) | *11.09.2025* |
| Status | *Fixed* |
| **Bug Description** | |
| URL | *https://github.com/qubic/core/blob/v1.258.1/src/contracts/Qx.h* |
| Summary | Attackers could exploit an integer overflow vulnerability by submitting excessively large values for `numberOfShares` and `price`. This overflow would occur when calculating the product of these two inputs, potentially allowing them to bypass the `if (qpi.invocationReward() < input.price * input.numberOfShares)` check. |
| Consequences | Attackers can drain all QUs and assets temporarily held in the QX contract by bypassing the sole security check. |
| Solution | Introduce new safe math functions with boundary checks. |
| Priority | High |
| Severity | Critical |

**Additional Notes, step-by-step Description:**

a. An attacker initiates a transaction with 1 QUs, manipulating `input.numberOfShares` and `input.price` to `9223372036854775807`.
b. This manipulation causes an overflow, resulting in `input.numberOfShares * input.price` evaluating to 1.
c. Consequently, the attacker's transaction circumvents security protocols and begins to drain QX funds.