BUG REPORT

SendToMany Missing Return After Invalid Amount

Mundus

03 Dec 2025

Bug Report: QVE-2025-0008

Bug ID	***QVE-2025-0008***
Finder	*Mundus team*
Date (reported)	*03.12.2025*
Status	*Found bug*
Bug Description	
URL	*https://github.com/qubic/core/blob/v1.268.1/src/contracts/QUtil.h#L569-L603*
Summary	After detecting invalid amounts and refunding, there's no return statement. Execution continues, which will likely fail and trigger another refund at the `exit: label`.
Consequences	Double refunding, SC loses funds
Solution	Add `return;` after the refund
Priority	Critical
Severity	Critical

Additional Notes, step-by-step Description

a. Attacker owns an address abcXYZ with 20M qu (an example)
b. With qubic-cli, attacker run a command to execute SendToManyV1
    - Parameters
        - Invocator: abcXYZ
        - To destination Id1 abcXYZ with amount 15M qu
        - To destination Id2 abcXYZ with amount -1M qu
    - Total amount: 15 - 1 = 14M qu
c. SendToManyV1 will do double refunding at line QUtil.h:601 and QUtil.h::643
d. Attacker will receive 14M qu more, so the abcXYZ's balance will be `20+14=34M` qu.