BUG REPORT

Vote Without Verification of Voter Identity

Mundus

27 Nov 2025

Bug Report: QVE-2025-0002

Bug ID	***QVE-2025-0002***
Finder	*Mundus team*
Date (reported)	*27.11.2025*
Status	*Found bug*
Bug Description	
URL	*https://github.com/qubic/core/blob/v1.268.1/src/contracts/QUtil.h#L1055-L1206*
Summary	Attackers can vote on behalf of any rich address without their consent.
Consequences	Attackers can manipulate the poll's voting results.
Solution	Need to verify if qpi.invocator() should be used instead
Priority	High
Severity	Critical

Additional Notes, step-by-step Description:

a. Attackers attend voting with a small fee.
b. Attackers vote with input.address = rich_user.
c. Balance check passes (rich_user has funds).
d. Vote is recorded for input.address with extreme voting power of rich_user, not the actual caller.