MSVAULT

Security Assessment and Code Audit

Mundus

25 Aug 2025

Rev 1

INTRODUCTION

The MSVAULT (Multi-Signature Vault) has been updated to support multiple digital assets and introduce a decentralized fee management system. It now allows for the secure, multi-party management of Qubic and up to eight other custom assets. The contract's operational fees are no longer static, as they can now be changed through a shareholder voting process, ensuring community-based governance over the economic model. This update expands the vault's utility and security, offering a more versatile and adaptable platform for pooled capital.

AUDIT PROCESS

Following considerations have been tested and reviewed by Mundus team:

- Reviewing google test files that are written by SC developer.
- Trying several attack vectors to exploit the SC.
- Ensuring contract logic meets the specifications.
- Thorough line-by-line manual review.

RESULTS

We identified a range of security issues in our assessment, from critical to minor. We recommend fixing them to meet security standards and best practices.

OVERVIEW

1. Project name: **MSVAULT**
2. Platform: **QUBIC SC system**
3. Is new SC deployment: **NO**
4. Is upgraded SC: **YES**
5. Project size: Medium
6. List of github commits to review:

    5211660a77c3c86df64f7dd09c5715f7f6a35c62

    b351f5644222f0d10c932afa7e23b53870f1bcfa

    c6d6547d17853eb99d343be0dd1daca9a4feecd3

    58b52f4291e50075600cbfa10ee97f5e2de7c1ed

    6b64e39c70b221d6bdefab03cf996ee9e9d386e0

    (https://github.com/qubic/core/pull/485/commits)

RESULTS SUMMARY

Total Issues	9
Critical	2
Major	0
Medium	4
Minor	3

AUDIT SCOPE

Filename	SHA	Latest commit
MsVault.h	58b52f4291e50075600cbfa10ee97f5e2de7c1ed	MsVault now supports assets
contract_msvault.cpp (google test)	6b64e39c70b221d6bdefab03cf996ee9e9d386e0	Add unit test for MsVault Asset

SUMMARY OF FINDINGS

ID	Title	Category	Severity
MSVAULT-01	Inconsistent fee handling among procedures	Logic	Critical
MSVAULT-02	Fee refund missing	Logic	Critical
MSVAULT-03	Missing returnCode for each procedure	Logic	Medium
MSVAULT-04	A local variable is prohibited	SC code convention	Medium
MSVAULT-05	Inconsistent fee between deposit vs depositAsset	Logic	Medium
MSVAULT-06	The API call needs a check to see if it failed or succeeded	Logic	Medium
MSVAULT-07	Signed/unsigned mismatch.	Logic	Minor
MSVAULT-08	Redundant codes	Logic	Minor
MSVAULT-09	Inconsistency in code style	Coding style	Minor

FINDINGS

MSVAULT-01 Inconsistent fee handling among procedures

- File(s) affected: MsVault.h
- Description: Fee should be handled as below
  - ➢ If a procedure cannot be processed, the fee should be refunded.
  - ➢ If a procedure is ready to be processed, the **live-XYZ-fee** should be applied.

  Currently, only **registerVault** has been handling the fee flow correctly.
- Recommendation: Ensure all procedures are re-examined for consistent fee handling.

MSVAULT-02 Fee refund missing

- File(s) affected: MsVault.h:941
- Description: Missing **qpi.transfer(qpi.invocator(), qpi.invocationReward()).**
- Recommendation: Either burn or refund

MSVAULT-03 Missing returnCode for each procedure

- File(s) affected: MsVault.h
- Description: Currently, MsVault procedures do not return a code in their results, making it challenging to determine the cause of any failures.
- Recommendation: To facilitate external API calls in checking and handling responses, every MsVault procedure's output structure should incorporate a returnCode member.

MSVAULT-04 A local variable is prohibited

- File(s) affected: MsVault.h:1751
- Description: As SC code convention, local variables are prohibited.
- Recommendation:

MSVAULT-05 Inconsistent fee between deposit vs depositAsset

- File(s) affected: MsVault.h:847
- Description: The **depositAsset** procedure is currently not applying any fee, it is inconsistent with **deposit**.
- Recommendation:

MSVAULT-06 The API call needs a check to see if it failed or succeeded

- File(s) affected: MsVault.h:908
- Description: The API call needs a check to see if it failed or succeeded
- Recommendation:

MSVAULT-07 Signed/unsigned mismatch

- File(s) affected: MsVault.h:857, 1066, 1229, 1292
- Description: Signed/unsigned mismatch.
- Recommendation:

MSVAULT-08 Redundant codes

- File(s) affected: MsVault.h:729-733
- Description: These lines are redundant and can be removed, even though they are not part of the PR's changes.
- Recommendation:

MSVAULT-09 Inconsistency in code style

- File(s) affected: MsVault.h:736
- Description: There is an inconsistency in code style regarding new line brackets.
- Recommendation: