Magic Square

SQRPaymentGateway
Smart Contract Audit Interim Report

Ver. 1.1
April 08, 2024

Table of Contents:

Table of Contents..... 2
Vulnerabilities found by type..... 2
1. SQRPaymentGateway.sol..... 3
Verification checksums..... 9

Vulnerabilities found by type:

INFO	1
WARNING	0
WARNING	0
TOTAL:	1

	ACKNOWLEDGED
High centralization risk.	
There is a high centralization risk due to the project structure.	

1. SQRPaymentGateway.sol

Contract methods analysis:

	INFO
initialize(address _newOwner, address _erc20Token, address _depositVerifier, uint256 _depositGoal, address _withdrawVerifier, uint256 _withdrawGoal, uint32 _startDate, uint32 _closeDate, address _coldWallet, uint256 _balanceLimit)	
In case startDate and endDate is initialized, consider checking that startDate < endDate	

_authorizeUpgrade(address newImplementation)
Vulnerabilities not detected

`changeBalanceLimit(uint256 _balanceLimit)`
Vulnerabilities not detected

`fetchFundItem(string memory userId)`
Vulnerabilities not detected

`getBalance()`
Vulnerabilities not detected

`balanceOf(string memory userId)`
Vulnerabilities not detected

`getHash(string memory value)`
Vulnerabilities not detected

`getDepositNonce(string memory userId)`
Vulnerabilities not detected

`getWithdrawNonce(string memory userId)`
Vulnerabilities not detected

`calculateRemainDeposit()`
Vulnerabilities not detected

`calculateRemainWithraw()`
Vulnerabilities not detected

`fetchTransactionItem(string memory transactionId)`
Vulnerabilities not detected

`getTransactionItem(string memory transactionId)`
Vulnerabilities not detected

`_setTransactionId(uint256 amount, string memory transactionId)`
Vulnerabilities not detected

`_deposit(string memory userId, string memory transactionId, address account, uint256 amount, uint32 nonce, uint32 timestampLimit)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens in

`deposit(string memory userId, string memory transactionId, address account, uint256 amount, uint32 nonce, uint32 timestampLimit)`
Vulnerabilities not detected

`verifyDepositSignature(string memory userId, string memory transactionId, address account, uint256 amount, uint32 nonce, uint32 timestampLimit, bytes memory signature)`
Vulnerabilities not detected

`depositSig(string memory userId, string memory transactionId, address account, uint256 amount, uint32 timestampLimit, bytes memory signature)`
Vulnerabilities not detected

`_withdraw(string memory userId, string memory transactionId, address to, uint256 amount, uint32 nonce, uint32 timestampLimit)`	
Vulnerabilities not detected	
TOKEN FLOW	Tokens out

`withdraw(string memory userId, string memory transactionId, address to, uint256 amount, uint32 nonce, uint32 timestampLimit)`
Vulnerabilities not detected

`verifyWithdrawSignature(string memory userId, string memory transactionId, address to, uint256 amount, uint32 nonce, uint32 timestampLimit, bytes memory signature)`
Vulnerabilities not detected

`withdrawSig(string memory userId, string memory transactionId, address to, uint256 amount, uint32 timestampLimit, bytes memory signature)`
Vulnerabilities not detected

Verification checksums

Contract name	Bytecode hash(SHA-256)
SQRPaymentGateway.sol	1f9710395750a9b26df40220aa8674901fc 9c795354a0e4d44064cf3becce89d