Storm Trade Audit Report

Severity levels

Critical - issue that can cause the significant loss of funds for the project or ability to steal client's money

Medium - issue that can cause loss of funds of an individual or protocol misbehavior

Low - code style, readability, usability, suggestions

Summary report by severity

Critical Severity

Ability to steal all funds from vault (deploy *PositionManager* with fake *vAMM*) (resolved)

1. We are sending `transfer_notification` with `op::increase_position` (for example) from user's wallet
2. Address for *vAMM* is not verified and the *PositionManager* created with this fake *vAMM*
3. Fake *vAMM* can send `activate_order` to *PositionManager* with any amount of money, the order is updated and now has **fake amount**
4. User cancels the order by the *PositionManager* and the *PositionManager* requests withdraw from vault
5. `request_withdraw_position` handler do not check vAMM used by the PositionManager and sends jettons to this user

Fixed by discovering vAMM address during the PositionManager init.

Medium severity

Jettons transfer_notification is not handled properly for invalid jettons (resolved)

Invalid `transfer_notification` is not handled properly. If user accidently sends invalid jetton his jettons would be lost.

Jettons transfer_notification is not handled properly for invalid jetton payloads or small value (resolved)

Invalid `transfer_notification` is not handled properly. If user accidently sends invalid payload with correct jetton, his tokens would be lost.

Low severity

Unnecessary preload_ref/preload_uint usage (resolved)

Example: there is no reason for using `preload` at the packers for PositionManager.

https://github.com/Tsunami-Exchange/ton-storm-contracts/blob/891f5cefbbeaf4440a9ae561414388d43f8dc249/contracts/position-manager/packers.fc#L12-L13

Users can mint referral item with any *Vault* address (resolved)

Minting regular referrals is allowed to anybody and requires vault address, vault address is not checked so it could be any. However, it does not cause any problems with current architecture.

I can recommend do not attach referral item to vault.

https://github.com/Tsunami-Exchange/ton-storm-contracts/blob/891f5cefbbeaf4440a9ae561414388d43f8dc249/contracts/referral-collection.fc#L94-L95

Not safe gas amount for trade_notification in *Vault (resolved)*

Sometimes `trade_notification` triggered with 0.11 TON gas amount, but it may require 0.104 (0.022 x2 for notifications + 0.06 for withdraw tokens) only for sending out messages.

https://github.com/Tsunami-Exchange/ton-storm-contracts/blob/891f5cefbbeaf4440a9ae561414388d43f8dc249/contracts/vault/handlers.fc#L299

Methods of audit

Visual check

Visual check of most of lines of code performed to cover obvious severities.

Access control analysis

We performed access checks penetration of every operation in the project.

Jettons flow

We analyzed where jettons are stored and how the transfer_notification is handled. Custom wallets also checked to satisfy the standard.

Message flags check

Check that every message sent with the correct flags.

Bounce handlers check

Ensure that every on_bounce handler reads no more than 256 bits of payload.