Fountain Finance

Feedbacks

contact@movebit.xyz

https://twitter.com/movebit_

Mon Apr 29 2024

1 Summary

During the audit, we identified 5 issues of varying severity, listed below.

ID	Title	Severity	Status
FCO-1	Centralization Risk	Major	Pending
FCO-2	Parameter Not Checked	Medium	Pending
FCO-3	May Cause Fountain to be Unavailable	Medium	Pending
FCO-4	Lack of Events Emit	Minor	Pending
FCO-5	Missing Param Check	Minor	Pending

2 Findings

FCO-1 Centralization Risk

Severity: Major

Status: Pending

Code Location:

sources/fountain_core.move#440-447

Descriptions:

Centralization risk was identified in the smart contract.

- Anybody can add the source, but only the `Admin` can withdraw any amount of source tokens.

Suggestion:

It is recommended to take measures to mitigate this issue.

FCO-2 Parameter Not Checked

Severity: Medium

Status: Pending

Code Location:

sources/fountain_core.move#304

Descriptions:

The initialized `PenaltyVault` requires the `max_penalty_rate` parameter to be less than or equal to `PENALTY_RATE_PRECISION`, but in the `update_max_penalty_rate` function, there is no check on the size of the `max_penalty_rate`, admin can make the `max_penalty_rate parameter` larger than `PENALTY_RATE_PRECISION`, causing users being penalized with excessive fines.

Suggestion:

It is recommended to add a check in the `update_max_penalty_rate` function.

FCO-3 May Cause Fountain to be Unavailable

Severity: Medium

Status: Pending

Code Location:

sources/fountain_core.move#164

Descriptions:

Before each `stake`, `unstake`, and other operations, we will call the `source_to_pool` function to release the tokens in the pool, if there are unreleased tokens, we will call the `release_resource` and `collect_resource` functions, `collect_resource` function will calculate the increased `cumulative_unit` according to `total_weigh` if the current time is bigger than the `latest_release_time` of `Fountain`, but at the beginning, `total_weigh` is equal to zero, so there will be an error here, resulting in the initial stake has been failed.

Suggestion:

It is recommended to confirm that this is compatible with the design concept.

FCO-4 Lack of Events Emit

Severity: Minor

Status: Pending

Code Location:

sources/fountain_core.move#284;

sources/fountain_core.move#307

Descriptions:

Some Functions in the contract lack appropriate events for monitoring sensitive operations, such as `update_flow_rate`, and `claim_penalty`, which could make it difficult to track sensitive actions or detect potential issues.

Suggestion:

It is recommended to emit events for those important functions.

FCO-5 Missing Param Check

Severity: Minor

Status: Pending

Code Location:

sources/fountain_core.move#82

Descriptions:

When calling the `new_fountain` function to create a fountain, there is a lack of checking the logical relationship of the parameters, for example, `min_lock_time` needs to be less than `max_lock_time`, and if there is no limit, the user may create a wrong fountain.

Suggestion:

It is recommended to add a check for the parameters.

Appendix 1

Issue Level

- **Informational** issues are often recommendations to improve the style of the code or to optimize code that does not affect the overall functionality.
- **Minor** issues are general suggestions relevant to best practices and readability. They don't post any direct risk. Developers are encouraged to fix them.
- **Medium** issues are non-exploitable problems and not security vulnerabilities. They should be fixed unless there is a specific reason not to.
- **Major** issues are security vulnerabilities. They put a portion of users' sensitive information at risk, and often are not directly exploitable. All major issues should be fixed.
- **Critical** issues are directly exploitable security vulnerabilities. They put users' sensitive information at risk. All critical issues should be fixed.

Issue Status

- **Fixed:** The issue has been resolved.
- **Partially Fixed:** The issue has been partially resolved.
- **Acknowledged:** The issue has been acknowledged by the code owner, and the code owner confirms it's as designed, and decides to keep it.