Fixed Point Solutions, LLC

Rari Vaults Assessment - Vault Initialization Module

2021/11/21
Prepared by: Kurt Barry

1. Scope

The following files and directories were audited based on the linked commits:
https://github.com/Rari-Capital/vaults/blob/80f6a5fc69b78e7a5092691db6f17325c93df5b2/src/modules/VaultCreationModule.sol

Note: the contract was renamed to `VaultInitializationModule` at a commit later than the one at which the audit was performed.

2. Limitations

No assessment can guarantee the absolute safety or security of a software-based system. Further, a system can become unsafe or insecure over time as it and/or its environment evolves. This assessment aimed to discover as many issues and make as many suggestions for improvement as possible within the specified timeframe. Undiscovered issues, even serious ones, may remain. Issues may also exist in components and dependencies not included in the assessment scope.

3. Findings

Findings and recommendations are listed in this section, grouped into broad categories. It is up to the team behind the code to ultimately decide whether the items listed here qualify as issues that need to be fixed, and whether any suggested changes are worth adopting. When a response from the team regarding a finding is available, it is provided.

Findings are given a severity rating based on their likelihood of causing harm in practice and the potential magnitude of their negative impact. Severity is only a rough guideline as to the risk an issue presents, and all issues should be carefully evaluated.

Severity Level Determination		Impact		
		High	Medium	Low
Likelihood	High	Critical	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Low

Issues that do not present any quantifiable risk (as is common for issues in the Code Quality category) are given a severity of **Informational**.

3.1 Security and Correctness

Findings that could lead to harmful outcomes or violate the intentions of the system.

SC.1 Vaults Can Be Permissionlessly Deployed Without Initialization

Severity: Low

Code Location:
[1]https://github.com/Rari-Capital/vaults/blob/de132f05f1354715d95c8357ce3de5b102510c95/src/VaultFactory.sol#L34
[2]https://github.com/Rari-Capital/vaults/blob/80f6a5fc69b78e7a5092691db6f17325c93df5b2/src/modules/VaultCreationModule.sol#L57

Description: The `deployVault` function is permissionless and deploys each vault to an address based solely on the vault's underlying token. This can be used to circumvent the initialization done by the `VaultCreationModule`, forcing governance to manually configure and initialize such vaults.

Response: Addressed in commit 650c7a2a838c9f34786547dba301a6a60bd84741.

3.2 Usability and Incentives

Findings that could lead to suboptimal user experience, hinder integrations, or lead to undesirable behavioral outcomes.

None.

3.3 Gas Optimizations

Findings that could reduce the gas costs of interacting with the protocol, potentially on an amortized or averaged basis.

None.

3.4 Code Quality

None.

4. Notes

This section contains general considerations for interacting with or maintaining the system and various conclusions reached or discoveries made during the course of the assessment. Whereas findings generally represent things for the team to consider changing, notes are more informational and may be helpful to those who intend to interact with the system.

None.