BURRA SEC

Centrifuge Security Review

Reviewed by: Goran Vladika

21st May - 23rd May, 2025

Centrifuge Security Review Report

Burra Security

May 27, 2025

Introduction

A time-boxed security review of the **Centrifuge** protocol was done by **Burra Security** team, focusing on the security aspects of the smart contracts.

Disclaimer

A smart contract security review can never verify the complete absence of vulnerabilities. This is a time, resource, and expertise-bound effort where we try to find as many vulnerabilities as possible. We can not guarantee 100% security after the review or even if the review will find any vulnerabilities. Subsequent security reviews, bug bounty programs, and on-chain monitoring are recommended.

About Burra Security

Burra Sec offers security auditing and advisory services with a special focus on cross-chain and interoperability protocols and their integrations.

About Centrifuge

Centrifuge V3 is an open, decentralized protocol for onchain asset management. Built on immutable smart contracts, it enables permissionless deployment of customizable tokenization products.

Build a wide range of use cases—from permissioned funds to onchain loans—while enabling fast, secure deployment. ERC-4626 and ERC-7540 vaults allow seamless integration into DeFi. Using protocol-level chain abstraction, tokenization issuers access liquidity across any network, all managed from one Hub chain of their choice.

Severity classification

Severity	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

Impact - The technical, economic, and reputation damage from a successful attack

Likelihood - The chance that a particular vulnerability gets discovered and exploited

Severity - The overall criticality of the risk

Informational - Findings in this category are recommended changes for improving the structure, usability, and overall effectiveness of the system.

Security Assessment Summary

***review commit hash* - 7762b38519e2f77cd0f03ff7e43ff765bfb630ad**

Scope

The following smart contracts were in the scope of the audit:

- src/hub/Hub.sol
- src/hub/HubHelpers.sol
- src/common/adapters/MultiAdapter.sol
- src/common/adapters/AxelarAdapter.sol
- src/common/adapters/WormholeAdapter.sol
- src/common/Gateway.sol
- src/common/GasService.sol

- src/misc/libraries/TransientArrayLib.sol
- src/misc/libraries/TransientBytesLib.sol

Findings Summary

ID	Title	Severity	Status
L-01	Deployer’s auth access on MultiAdapter should be revoked	Low	Resolved
L-02	Missing setter for hubHelpers in Hub	Low	Resolved

Detailed Findings

[L-01] Deployer’s auth access on MultiAdapter should be revoked

Target

- CommonDeployer.s.sol

Severity:

- Impact: Medium
- Likelihood: Low

Description:

As part of the deployment process deployer account is initially set as an admin on the protocol contracts. Then this access is revoked on most of the contracts, but not on the multiAdapter:

```
    function removeCommonDeployerAccess(address deployer) public {
        if (root.wards(deployer) == 0) {
            return; // Already removed. Make this method idempotent.
        }

        guardian.file("safe", address(adminSafe));

        root.deny(deployer);
        gateway.deny(deployer);
        tokenRecoverer.deny(deployer);
        messageProcessor.deny(deployer);
        messageDispatcher.deny(deployer);
```

That means deployer account keeps their admin access. If attacker would gain access over this account, there could be a lot of damage done to the protocol.

Recommendation:

Revoke deployer's auth access from the multiAdapter as well:

```
        multiAdapter.deny(deployer);
```

Client:

Fixed in PR-399

BurraSec:

Fix verified

[L-02] Missing setter for hubHelpers in Hub

Target

- Hub.sol

Severity:

- Impact: Medium
- Likelihood: Low

Description:

Hub contract has a storage variable which stores the address of the hubHelpers contract. Even though hubHelpers variable is not immutable, its value can be set only in constructor. If hubHelpers address changed, ie. due to the updated implementation of some of the hub actions, there would be no way to point the Hub contract to the new hubHelpers address. This increases the complexity of protocol maintenance.

Recommendation:

Add the option to update the hubHelpers in the file function.

Client:

Fixed in PR-399

BurraSec:

Fix verified