Arrakis Finance Audit

March 07, 2022

WATCHPUG

Table of Contents

Summary

This report has been prepared for **Arrakis Finance** smart contracts, to discover issues and vulnerabilities in the source code of their Smart Contract as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Overview

Project Summary

Project Name	**Arrakis Finance**
Codebase	https://github.com/ArrakisFinance/vault-v1-periphery https://github.com/ArrakisFinance/vault-v1-core
Commit	e832b6989e4a056485826cdaf511a3896c5b3a4c d2d879e9a25f24d77a7a0a01b3681f04621a7cdb
Language	Solidity

Audit Summary

Delivery Date	**Mar 07, 2022**
Audit Methodology	**Static Analysis, Manual Review**
Total Isssues	**4**

AR-N1: Unused imports

Informational

Issue Description

vault-v1-periphery - contracts/interfaces/IArrakisV1RouterStaking.sol

Identifier "IArrakisVaultV1" is unused.

vault-v1-core - contracts/ArrakisVaultV1.sol

Identifier "IUniswapV3Pool" is unused.

Status

✓ Fixed

Fixed in commit: 05063f495b9618fd7152bc948183f00042c88d4a (vault-v1-periphery) and 2d60d68414b5d09e59ff5ef49ce1cac05299ebb0 (vault-v1-core).

AR-N2: Outdated comments should be updated

Informational

Issue Description

contracts/ArrakisVaultV1.sol

There are some outdated comments from the G-UNI era, which should be updated to avoid misunderstanding.

Specifically, for `withdrawManagerBalance()` and `withdrawArrakisBalance()`.

Status

✓ **Fixed**

Fixed in commit: 2d60d68414b5d09e59ff5ef49ce1cac05299ebb0 (vault-v1-core).

AR-N3: toggleRestrictMint() should be idempotent

Informational

Issue Description

contracts/abstract/ArrakisVaultV1Storage.sol#L147-L153

```
function toggleRestrictMint() external onlyManager {
    if (restrictedMintToggle == 11111) {
        restrictedMintToggle = 0;
    } else {
        restrictedMintToggle = 11111;
    }
}
```

If the `toggleRestrictMint()` function is called twice in a row, the result can be different than expected, especially if there are multiple addresses allowed to call it, which should not the case for this function, since there is only one manager.

Recommendation

Consider adding a parameter for the desired status so that this function can be idempotent, or consider having two separate functions to enable and disable restrictedMint, just like pause() and unpause().

Status

ⓘ Acknowledged

AR-N4: Using constant instead of literal can improve readability

Informational

Issue Description

contracts/abstract/ArrakisVaultV1Storage.sol#L147-L153

```
function toggleRestrictMint() external onlyManager {
    if (restrictedMintToggle == 11111) {
        restrictedMintToggle = 0;
    } else {
        restrictedMintToggle = 11111;
    }
}
```

Recommendation

Consider adding a constant named RESTRICTED_MINT_ENABLED with the value being 11111, and use the constant to improve readability.

Status

✓ Fixed

Fixed in commit: 2d60d68414b5d09e59ff5ef49ce1cac05299ebb0 (vault-v1-core).

Appendix

Timeliness of content

The content contained in the report is current as of the date appearing on the report and is subject to change without notice, unless indicated otherwise by WatchPug; however, WatchPug does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following publication.

Disclaimer

This report is based on the scope of materials and documentation provided for a limited review at the time provided. Results may not be complete nor inclusive of all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Smart Contract technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. A report does not indicate the endorsement of any particular project or team, nor guarantee its security. No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, we disclaim all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate. FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.