Security Audit Report

AshPerp vault
MultiversX smart contract

by ARDA

on June 1, 2024

Table of Contents

Disclaimer

The report makes no statements or warranties, either expressed or implied, regarding the security of the code, the information herein or its usage. It also cannot be considered as a sufficient assessment regarding the utility, safety and bugfree status of the code, or any other statements.

This report does not constitute legal or investment advice. It is for informational purposes only and is provided on an "as-is" basis. You acknowledge that any use of this report and the information contained herein is at your own risk. The authors of this report shall not be liable to you or any third parties for any acts or omissions undertaken by you or any third parties based on the information contained herein.

Terminology

Code: The code with which users interact.

Inherent risk: A risk for users that comes from a behavior inherent to the code's design.

Inherent risks only represent the risks inherent to the code's design, which are a subset of all the possible risks. **No inherent risk doesn’t mean no risk.** It only means that no risk inherent to the code's design has been identified. Other kind of risks could still be present. For example, the issues not fixed incur risks for the users, or the upgradability of the code might also incur risks for the users.

Issue: A behavior unexpected by the users or by the project, or a practice that increases the chances of unexpected behaviors to appear.

Critical issue: An issue intolerable for the users or the project, that must be addressed.

Major issue: An issue undesirable for the users or the project, that we strongly recommend to address.

Medium issue: An issue uncomfortable for the users or the project, that we recommend to address.

Minor issue: An issue imperceptible for the users or the project, that we advise to address for the overall project security.

Objective

Our objective is to share everything we have found that would help assessing and improving the safety of the code:

1. The **inherent risks** of the code, labelled R1, R2, etc.
2. The **issues** in the **code**, labelled C1, C2, etc.
3. The **issues** in the **testing** of the code, labelled T1, T2, etc.
4. The **issues** in the **other** parts related to the code, labelled O1, O2, etc.
5. The **recommendations** to address each issue.

Audit Summary

Initial scope

- **Repository:** https://github.com/ashswap/ash-tinder-sc
- **Commit:** `a224e76dc6007b1443875c876ab161a3ac6ae911`
- **MultiversX smart contract path:** ./contracts/vault/

Final scope

- **Repository:** https://github.com/ashswap/ash-tinder-sc
- **Commit:** `37feaa4cba1c0f224d39c86ec8ae08d95ad04a82`
- **MultiversX smart contract path:** ./contracts/vault/

4 inherent risks in the final scope

0 issue in the final scope

17 issues reported in the initial scope and 0 remaining in the final scope:

Severity	Reported			Remaining		
	Code	Test	Other	Code	Test	Other
Critical	0	0	0	0	0	0
Major	3	0	0	0	0	0
Medium	11	0	0	0	0	0
Minor	3	0	0	0	0	0

Inherent Risks

R1: Users might lose part or all the money they deposit in the vault.

This is because the vault would lose money in case traders have made more profits than losses since the moment the user would have entered the vault.

R2: Users might lose more money or earn less money than they should.

This is because liquidations, take profits, stop losses, order closures are executed by the oracle bots that, for example, (1) could choose a price worse than the market price, or (2) could miss a moment where the execution should have happened.

R3: Users have no guarantee that the insurance funds will cover all their losses.

Appeared in intermediary commit: `e2647d578a3e294f2623cf13156bc1730884b7ec`

This is because there may be less tokens in the insurance funds than necessary to pay all traders' positive PnL. More precisely, the insurance funds is composed of:

- A percentage of the trader's negative PnL.
- Additional deposits that the AshPerp team may decide to provide.

Therefore if traders make big profits, eventually the insurance funds will be exhausted. Moreover, the AshPerp team can deplete the insurance funds at any time by any amount.

R4: The owner can withdraw funds from the insurance funds.

Appeared in intermediary commit: `e2647d578a3e294f2623cf13156bc1730884b7ec`

This is because the owner has the ability to withdraw any amount from the insurance funds at any time. Therefore there is no guarantee that the insurance funds will fully be used to protect against the Vault's losses, i.e. traders' positive PnL.

Code Issues & Recommendations

Since the code is not open-source, only the remaining issues are published.