Security Audit Report

AshPerp price-aggregator (2)
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:** `e2647d578a3e294f2623cf13156bc1730884b7ec`
- **MultiversX smart contract path:** ./contracts/price_aggregator/

Final scope

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

2 inherent risks in the final scope

0 issue in the final scope

2 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	0	0	0	0	0	0
Medium	1	0	0	0	0	0
Minor	1	0	0	0	0	0

Inherent Risks

R1: An oracle bot might fulfill an order with delay or not at all.

This is because:

- At most `5` orders can be fulfilled in each block and thus the delay in fulfillment will appear as soon as more than `5` orders appear per block.
- The Hatom oracle that is used to do a sanity check on the price might fail or be too far away from the price of the oracle bot and therefore the order fulfillment would fail.

R2: An oracle bot might not be able to do a sanity check on the price used to fulfill an order.

This is because the Hatom oracle might not provide a price for the token in question.

Code Issues & Recommendations

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