Security Audit Report

Hatom booster-v1
MultiversX smart contract

by ARDA

on November 26, 2023

Table of Content

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/HatomProtocol/hatom-rewards-booster/
- **Commit:** `254d80c4d3c90726141c3cac5a182d933f30df8a`
- **MultiversX smart contract path:** ./rewards-booster/

Final scope

- **Repository:** https://github.com/HatomProtocol/hatom-rewards-booster-v1
- **Commit:** `31daab279523188759fdc5ac3c69425490bc67aa`
- **MultiversX smart contract path:** ./rewards-booster/

3 inherent risks in the final scope

0 issue in the final scope

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

Severity	Reported			Remaining		
	Code	Test	Other	Code	Test	Other
Critical	1	0	0	0	0	0
Major	4	0	0	0	0	0
Medium	9	0	0	0	0	0
Minor	6	0	0	0	0	0

Inherent Risks

R1: Users may not be able to claim rewards as HTM if they claim too late.

This is because the contract has only a limited amount of rewards that can be converted to HTM.

Example: Let's say that if Alice claims now, she would be able to claim rewards as HTM. However, if she rather decides to claim one week later, it is possible that she may not be able to claim rewards as HTM anymore, for instance in the following cases:

- Other users have claimed rewards as HTM during the week, and there are not enough remaining rewards that can be converted to HTM for Alice.
- No other users claimed during the week, but Alice's rewards have increased and may have now exceeded the contract's amount of rewards that can be converted to HTM.

R2: Users might earn less rewards over a period of time depending on when they claim during that period.

This is because the computation of rewards of a user since his last interaction is based on values that increase / decrease over time:

- the price of the HTM he staked in the Booster,
- the price of supply tokens he deposited as collateral in the Controller,
- the capping of the compliance to 1.

R3: Users might earn less rewards than they expect.

This is because the penalty applied to the user's rewards is determined by the relative prices of staked and collateral tokens, which are provided by oracle

sources, and there is no guarantee that these sources will not be manipulated, will function continuously, and will provide accurate data.

Here are some sources of errors in prices used in the Booster:

- There is no guarantee that ESDT prices provided by Hatom Oracle to the Booster are accurate, because they are obtained by aggregating prices given by off-chain bots, which can be manipulated, stop functioning or provide inaccurate data. Additionally, although the Oracle may partially mitigate this risk by not providing its price if it is too far from the xExchange safe price, this mitigation mechanism might not always be activated.
- There is no guarantee that each price used in the Booster is up-to-date, because instead of asking the Hatom Oracle to compute a fresh price, the Booster uses the price which it last saved, or the last saved price in Hatom Oracle. Therefore, if there are no interactions for some time with Hatom Oracle, prices used in the Booster would progressively become outdated.

Code Issues & Recommendations

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