Security Audit Report

Hatom wrapped-tao
smart contract

by ARDA

on March 21, 2024

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

Inherent risk: A risk for users that comes from a behavior inherent to the smart contract design.

Inherent risks only represent the risks inherent to the smart contract 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 smart contract 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 smart contracts deployed as upgradeable 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.

Audit Summary

Scope of initial audit

- **Repository:** https://github.com/HatomProtocol/hatom-wrapped-tao
- **Commit:** `b4bb3845ed62061dbf3582939155a1f82da36652`
- **Path to Smart contract:** `./wrapped-tao/`

Scope of final audit

- **Repository:** https://github.com/HatomProtocol/hatom-wrapped-tao
- **Commit:** `4f147af38bf4d39f77e49eff6735fe96665c894f`
- **Path to Smart contract:** `./wrapped-tao/`

Report objectives

1. Reporting all **inherent risks** of the smart contract.
2. Reporting all **issues** in the smart contract **code**.
3. Reporting all **issues** in the smart contract **test**.
4. Reporting all **issues** in the **other** parts of the smart contract.
5. Proposing **recommendations** to address all issues reported.

2 inherent risks in the final commit

1 issue in the final commit

7 issues reported from the initial commit and 1 remaining in the final commit:

Severity	Reported			Remaining		
	Code	Test	Other	Code	Test	Other
Critical	0	0	0	0	0	0
Major	2	0	0	0	0	0
Medium	1	1	0	0	0	0
Minor	3	0	0	1	0	0

Inherent Risks

R1: Users might not receive the funds they tried to bridge.

This is because a user has to trust that a bridge relayer will execute his request in due time and will bridge the correct amount to the correct address, both for bridging funds from MultiversX and to MultiversX.

R2: Users might not be able to get back 1 TAO per 1 wTAO.

This is because any relayer is allowed to mint wTAO, and there is no guarantee that these wTAO correspond to TAO that were deposited on Bittensor's side of the bridge. For example, let's say that users currently have 1000 wTAO on MultiversX, and that one relayer gets compromised. Then, this relayer mints 1000 wTAO and bridges them back on Bittensor, thus obtaining all the available TAO. From then on, users cannot bridge their wTAO to Bittensor and get back their TAO.

Code Issues & Recommendations

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

C6: Unused error message

Appeared in intermediary commit: `4f147af38bf4d39f77e49eff6735fe96665c894f`

Severity: Minor **Status:** Won't fix

Location

`wrapped-tao/src/errors.rs`

Description

The error message `ERROR_MINTER_IS_REWARDS_MANAGER` is unused.

Recommendation

We suggest deleting `ERROR_MINTER_IS_REWARDS_MANAGER`.

Test Issues & Recommendations

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