0x Guard

Smart contracts security assessment

Final report

Tariff: Top

Astromarket

June 2022

0xguard.com

hello@0xguard.com

Contents

Introduction

The report has been prepared for the Astromarket team.

Name	Astromarket
Audit date	2022-05-29 - 2022-06-03
Language	Rust
Platform	NEAR

Contracts checked

Name	Address
Contract	

Procedure

We perform our audit according to the following procedure:

Automated analysis

- Scanning the project's smart contracts with several publicly available automated analysis tools
- Manual verification (reject or confirm) all the issues found by the tools

Manual audit

- Manually analyze smart contracts for security vulnerabilities
- Smart contracts' logic check

Classification of issue severity

High severity	High severity issues can cause a significant or full loss of funds, change of contract ownership, major interference with contract logic. Such issues require immediate attention.
Medium severity	Medium severity issues do not pose an immediate risk, but can be detrimental to the client's reputation if exploited. Medium severity issues may lead to a contract failure and can be fixed by modifying the contract state or redeployment. Such issues require attention.
Low severity	Low severity issues do not cause significant destruction to the contract's functionality. Such issues are recommended to be taken into consideration.

Issues

High severity issues

No issues were found

Medium severity issues

1. Wrong storage management (Contract)

In the contract, there are no checks on transfer results. It is a better practice to check all results for all promises.

Team response: This function isn't now availableIt will be changed and then will be used in the future.so we don't use bid function of contract now(just structure of future)

2. Wrong interactiom with royalty (Contract)

In the functions `buy()` and `internal_accept_offer()` there is an interaction with the `nft_transfer_payout()` function of an NFT. This function returns as a result an array of royalty receivers. Interactions with this array are performed under the assumption that it contains information about the amount for a seller of an NFT, but there is no such guarantee.

Team response: We will verify contact if it inherits nep-171 standard before importing nft smart contract on our market contract. Also we don't care about how much the contract's royalty is set. If we found issues some contract is scammable, then we will stop verification and will remove the collection from our market.

3. No checking on transfer results (Contract)

In the contract, there are no checks on transfer results. It is a better practice to check all results for all promises.

Team response: There are checking part on nft transfer, but not have in only near token transfer.It isn’t need actually, because near token is native token and all funds will be sent to market before trading, so there will be enough funds in contract always.

Low severity issues

1. Max fee (Contract)

The owner can set fees of up to 99.99% to the value. It is a better practice to set a lower border for commission.

Team response: If there are scam NFTs on market, our contract owner(Ted) can set a max fee for the collection.

Conclusion

Astromarket Contract contract was audited. 3 medium, 1 low severity issues were found.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability)set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without 0xGuard prior written consent.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts 0xGuard to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

0x Guard