Code Issues 4 Pull requests Actions Projects Security Insight

Edit New issue Jump to bottom

Treasure Marketplace Contract Review ac31264 #25

Closed **fulldecent** opened this issue on Mar 6, 2022 · 3 comments

fulldecent commented on Mar 6, 2022 • edited Contributor

Treasure Marketplace Contract Review
William Entriken
Delivered 2022-03-06

Thank you for the opportunity to participate in this code review!

Review scope

This is a review of Treasure Marketplace, pre-release version. Code was published at `ac31264` with SHA-1 hash `ac31264ac2973de946dc397d01c2cf8118ce9616` .

The scope of review included code-level review (human reading source code), automated code review, (computer reading source code). Due to limitations of the engagement, the review does not include unit testing (computer running small-scope tests), and functional testing (human using compiled program).

The review was performed for the purpose of comparing Treasure Marketplace against known vulnerabilities of the deployed Treasure Marketplace contract, the plain English meaning of comments and function names, and a general understanding of NFT marketplaces. Any deviation from this standard, or deficiency against relevant best programming practices would be an in-scope review finding.

Sensitivity was set as "anything we should fix or that you wouldn't want a million people to read".

Review exclusions

Open Zeppelin Contacts were specifically excluded from the scope. Although certain notes about the contracts used are provided below.

Quality and correctness of automated testing approaches and deployment strategy is excluded from the scope.

Each finding is listed and is organized by topic. Critical findings that are not resolved are marked with the bomb symbol (💣) and other unresolved material findings are marked with the warning symbol (⚠️). Resolved and less-than-material findings have no emoji marking.

Undisclosed powers of owner

These findings are related to features that the owner has control over which may pose risks to other users.

⚠️ Owner may frontrun and take 100% of fees

[💣 Owner may steal customer NFTs](#6)

⚠️ Owner can rugpull with upgrade

Marketplace design

These are fundamental design issues. Fixings these will affect the smart contract as well as the front-end application.

💣 Updating the payment token changes the commitments on behalf of sellers without their consent

💣 Seller unable to cancel listing

💣 Owner can harm sellers by pausing contract

💣 Expiration times can be are much longer than specified

[updateListing does not allow to increase price](#17)

[There is no meaningful difference between createListing and updateListing](#18)

Implementation details

These findings affect only the smart contract and not any other applications.

⚠️ Package management uses ranges

[Solidity version is unsupported](#9)

[Gas inefficient storage of listings](#10)

[Unsemantic reference to payment token](#12)

[NFT registration could obviate need for using ERC-165 introspection](#13)

[Opportunities for inlining code](#19)

[_buyItem implementation is fragile to reentrancy](#23)

#30

Code style

There findings relate to only the way that the code is presented.

⚠️ Deprecated wording

[NatSpec documentation is missing](#4)

[Code does not follow the Solidity style guide](#24)

☺ 👍 6 ❤️ 8

minebuu commented on Mar 6, 2022

Respect you. I learned a lot from the issues you submitted.

☺ ❤️ 5

ghoul-sol commented on Mar 12, 2022 • edited ▾ Collaborator

I believe all findings have been addressed and the issue can be closed.

☺

ghoul-sol commented on Mar 12, 2022 Collaborator

If anything is missing, feel free to reopen.

☺

ghoul-sol closed this as completed on Mar 12, 2022

Assignees

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants